

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-285623

(P2001-285623A)

(43) 公開日 平成13年10月12日 (2001. 10. 12)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 N 1/387		H 0 4 N 1/387	5 B 0 5 7
G 0 6 T 1/00	5 0 0	G 0 6 T 1/00	5 0 0 B 5 C 0 6 3
G 1 0 L 11/00		G 1 0 L 9/00	E 5 C 0 7 6
H 0 4 N 7/08		H 0 4 N 7/08	Z
7/081			

審査請求 未請求 請求項の数31 O L (全 34 頁)

(21) 出願番号 特願2000-263872(P2000-263872)

(22) 出願日 平成12年8月31日 (2000. 8. 31)

(31) 優先権主張番号 特願平11-280652

(32) 優先日 平成11年9月30日 (1999. 9. 30)

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願2000-16285 (P2000-16285)

(32) 優先日 平成12年1月25日 (2000. 1. 25)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 村谷 博文

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

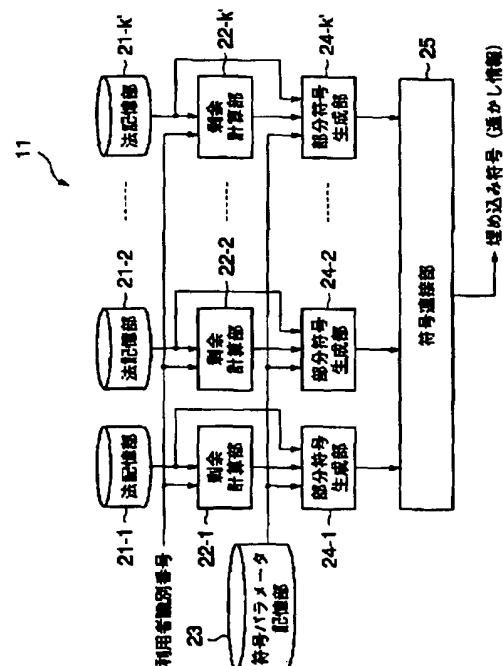
最終頁に続く

(54) 【発明の名称】 埋め込み符号生成方法及び装置、埋め込み符号検出方法及び装置並びに電子透かし埋め込み装置及び電子透かし検出装置

(57) 【要約】

【課題】 結託攻撃への耐性を持ち、利用者総数や結託者総数が大きな場合においても、コンテンツの品質劣化を極力抑えた透かし情報として埋め込まれる埋め込み符号生成装置を提供する。

【解決手段】 剰余計算部22-1, 22-2, ..., 22-k'により利用者IDに対して法記憶部21-1, 21-2, ..., 21-k'に記憶された互いに素の関係にある複数の整数を法とする剰余をそれぞれ求め、これらの剰余及び符号化パラメータ記憶部23に記憶されたパラメータに基づいて、成分符号生成部24-1, 24-2, ..., 24-k'により所定のビット数を一単位とする連続した1の列及び0の列で構成される成分符号をそれぞれ生成し、これらの各成分符号を接続部25で接続して、透かし情報を構成する埋め込み符号を生成する。



1

【特許請求の範囲】

【請求項 1】所定のコンテンツに埋め込まれるべき埋め込み符号を生成する埋め込み符号生成方法において、前記コンテンツを利用する利用者の利用者識別番号に対して、互いに素の関係にある複数の整数を法とする複数の剰余を計算する剰余計算ステップと、前記剰余計算手段により求められた各剰余を表す複数の成分符号を生成する成分符号生成ステップと、前記成分符号生成手段により生成された各成分符号を連結して前記埋め込み符号を生成する接続ステップとを具備する埋め込み符号生成方法。

【請求項 2】所定のコンテンツに埋め込まれるべき埋め込み符号を生成する埋め込み符号生成装置において、前記コンテンツを利用する利用者の利用者識別番号に対して、互いに素の関係にある複数の整数を法とする複数の剰余を計算する剰余計算手段と、前記剰余計算手段により求められた各剰余を表す複数の成分符号を生成する成分符号生成手段と、前記成分符号生成手段により生成された各成分符号を連結して前記埋め込み符号を生成する接続手段とを具備する埋め込み符号生成装置。

【請求項 3】前記成分符号生成手段は、前記複数の成分符号として所定のビット数を一単位とする連続した 1 の列及び 0 の列で構成される符号を生成する請求項 2 記載の埋め込み符号生成装置。

【請求項 4】所定のコンテンツに埋め込まれた、複数の成分符号を接続した埋め込み符号を検出する埋め込み符号検出方法において、前記埋め込み符号を前記複数の成分符号に分割する符号分割ステップと、分割された各成分符号をそれぞれ復号して予め定められた互いに素の関係にある複数の整数を法とする 2 つの剰余からなる複数の剰余対を得る成分符号復号ステップと、前記複数の剰余対から前記コンテンツに対して結託攻撃を行った結託者の利用者識別番号を計算する結託者番号計算ステップとを具備する埋め込み符号検出方法。

【請求項 5】所定のコンテンツに埋め込まれた複数の成分符号を接続した埋め込み符号を検出する埋め込み符号検出装置において、前記埋め込み符号を前記複数の成分符号に分割する符号分割手段と、分割された各成分符号をそれぞれ復号して予め定められた互いに素の関係にある複数の整数を法とする 2 つの剰余からなる複数の剰余対を得る成分符号復号手段と、前記複数の剰余対から前記コンテンツに対して結託攻撃を行った結託者の利用者識別番号を計算する結託者番号計算手段とを具備する埋め込み符号検出装置。

【請求項 6】前記複数の成分符号は、所定のビット数を一単位とする連続した 1 の列及び 0 の列で構成される請

2

求項 5 記載の埋め込み符号検出装置。

【請求項 7】前記複数の剰余対から結託の有無を判定する結託判定手段をさらに有し、前記結託者番号計算手段は該結託判定手段により結託があると判定されたとき前記結託者の利用者識別番号を計算する請求項 5 記載の埋め込み符号検出装置。

【請求項 8】前記結託者番号計算手段は、入力された k' 個の剰余対の各々から一方の剰余を選択して k' 個の剰余の組 $(R_1, R_2, \dots, R_{k'})$ を生成する剰余選択部と、

前記剰余選択部により生成された k' 個の剰余の組から選択された相異なる k 個の剰余 (S_1, S_2, \dots, S_k) から中国剰余定理に従って結託者の利用者識別番号 u の候補を計算する中国剰余定理部と、

前記剰余選択部により生成された k' 個の剰余の組から前記 k 個の剰余を選択して前記中国剰余定理部に渡し、前記中国剰余定理部により計算された結託者の利用者識別番号候補 u の候補から該結託者の利用者識別番号を特定して出力する一貫性検査部とを含み、

前記一貫性検査部は、前記剰余選択部により生成された k' 個の剰余の組から前記 k 個の剰余を選択する選択処理と、前記中国剰余定理部により計算された結託者の利用者識別番号 u の候補と残りの $(k' - k)$ 個の剰余のうちの所定個数 (y) の剰余との間に $R_i = u \bmod p_i (i = i_1, i_2, \dots, i_z)$ の関係が成立するか否かを判定する判定処理と、該判定処理により前記関係が成立する場合に結託者の利用者識別番号として出力する出力処理とを有し、

前記関係が成立しない場合には前記剰余選択部により生成された k' 個の剰余の組から前記選択処理により新たな組み合わせの k 個の剰余 (S_1, S_2, \dots, S_k) を選択して前記判定処理を行い、全ての組み合わせの k 個の剰余 (S_1, S_2, \dots, S_k) に対して前記関係が成立しない場合には前記剰余選択部に対して新たな k' 個の剰余の組を要求して、前記関係が成立するまで前記選択処理及び判定処理を繰り返す請求項 5 記載の埋め込み符号検出装置。

【請求項 9】入力された利用者識別番号に対応して複数の整数要素の組を計算する計算手段と、

所定個数の利用者識別番号に対して前記計算手段により計算される全ての整数要素の組を表現可能な k' 個の成分符号のうちの k 個の組み合わせが前記利用者識別番号を一意に表現できる成分符号を前記各整数要素に対応してそれぞれ生成する成分符号生成手段と、

前記成分符号生成手段により生成された各成分符号を連結して埋め込み符号を生成する接続手段とを具備し、前記 k' は、3 以上の正整数を c 、1 以上の正整数を z 、前記埋め込み符号の検出時に前記各成分符号から検出できる前記整数要素の個数を q として、 $c(k+z)/q$ 以上となるように決定されている埋め込み符号生成装

3

置。

【請求項 10】前記所定個数の利用者識別番号に対して前記計算手段により計算される各整数要素のとりうる値の個数を $p_i (i = 1, 2, \dots, k')$ とし、前記埋め込 *

$$\left[1 - \prod_{i=1}^z \left\{ 1 - \left(1 - \frac{1}{p_i} \right)^c \right\} \right]^{c(k+z)2^{Ct+z}2^{kz}} \geq 1 - \frac{\varepsilon}{2} \quad (1)$$

の条件を満たすように設定されている請求項 9 記載の埋め込み符号生成装置。 10 ※する請求項 9 記載の埋め込み符号生成装置。

【請求項 11】前記計算手段は、前記入力された利用者識別番号に対応して互いに素の関係にある複数の整数を法とする剰余の組を前記整数要素の組として計算する請求項 9 記載の埋め込み符号生成装置。

【請求項 12】前記計算手段は、前記入力された利用者識別番号に対応して平行移動によって定義される同値類に属する要素の番号の組を前記整数要素の組として計算※

$$k' = \frac{c}{2}(k+z) \leq \frac{p^t - 1}{p - 1} \quad (2)$$

の条件をさらに満たす請求項 9 記載の埋め込み符号生成装置。

【請求項 14】所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能な k' 個の成分符号のうちの k 個の組み合わせが利用者識別番号を一意に表現できる成分符号であって、入力された利用者識別番号に対応して計算された整数要素の組に対応して生成された部分を接続した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、抽出された各成分符号に分割する符号分割手段と、分割された各成分符号をそれぞれ復号する成分符号復号手段と、

★ 【数 3】

$$\left[1 - \prod_{i=1}^z \left\{ 1 - \left(1 - \frac{1}{p_i} \right)^c \right\} \right]^{c(k+z)2^{Ct+z}2^{kz}} \geq 1 - \frac{\varepsilon}{2} \quad (1)$$

の条件を満たすように設定されている請求項 14 記載の埋め込み符号検出装置。

【請求項 16】前記整数要素の組は、前記利用者識別番号に対応して計算された互いに素の関係にある複数の整数を法とする剰余の組である請求項 14 記載の埋め込み符号検出装置。

【請求項 17】前記整数要素の組は、前記利用者識別番号に対応して計算された平行移動によって定義される同

$$k' = \frac{c}{2}(k+z) \leq \frac{p^t - 1}{p - 1} \quad (2)$$

の条件をさらに満たす請求項 14 記載の埋め込み符号検 50 出装置。

4

*み符号の検出時に想定される検出誤り率を ε としたとき、前記 k' は、

【数 1】

【請求項 13】前記計算手段は、前記入力された利用者識別番号に対応して平行移動によって定義される同値類に属する要素の番号の組を前記整数要素の組として計算するものであり、

前記 $p_i (i = 1, 2, \dots, k')$ を同一の正整数 p とし、

【数 2】

★各成分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、

前記 k' は、3 以上の正整数を c 、1 以上の正整数を z 、前記埋め込み符号の検出時に前記各成分符号から検出できる前記整数要素の個数を q とし、 $c(k+z)/q$ 以上となるように決定されている埋め込み符号検出装置。

【請求項 15】前記所定個数の利用者識別番号に対して計算される各整数要素のとりうる値を $p_i (i = 1, 2, \dots, k')$ とし、前記埋め込み符号の検出時に想定される検出誤り率を ε としたとき、前記 k' は、

★ 【数 3】

☆値類に属する要素の番号の組である請求項 14 記載の埋め込み符号検出装置。 40

【請求項 18】前記整数要素の組は、前記利用者識別番号に対応して計算された平行移動によって定義される同値類に属する要素の番号の組であり、

前記 $p_i (i = 1, 2, \dots, k')$ を同一の正整数 p とし、

【数 4】

5

【請求項19】所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能な k' 個の成分符号のうちの k 個の組み合わせが利用者識別番号を一意に表現できる成分符号であって、入力された利用者識別番号に対応して計算された整数要素の組に対応して生成された部分を接続した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、抽出された各成分符号に分割する符号分割手段と、分割された各成分符号をそれぞれ復号する成分符号復号手段と、

各成分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、

前記成分符号復号手段は、前記各成分符号をブロックに分割するブロック分割部と、該ブロック毎にブロック内の“1”のビット数を計数する計数部と、該計数部で得られた計数値が第1の閾値を越えているか否かを判定する第1の判定部と、前記計数値が第2の閾値に満たないか否かを判定する第2の判定部と、前記第1の判定部で第1の閾値を越えていると判定された最小のブロックを決定する最小位置決定部と、前記第2の判定部で第2の閾値に満たないと判定された最大のブロックを決定する最大位置決定部とを有し、前記最小位置決定部及び最大位置決定部の決定結果を復号結果として出力する埋め込み符号検出装置。

【請求項20】前記利用者識別番号の割り当て要求に対して、複数の利用者識別番号候補の中から前記結託者の利用者識別番号として誤検出される可能性のより低い一つの候補を選択し、該選択した利用者識別番号を前記利用者を特定する利用者特定情報に対して割り当てる利用者識別番号割り当て手段をさらに具備する請求項2記載の埋め込み符号生成装置。

【請求項21】前記利用者識別番号割り当て手段は、前記複数の利用者識別番号候補を一つずつシーケンシャルに入力して、該候補について前記結託者の利用者識別番号として誤検出される可能性の高低を判定し、該可能性が低いと判定した利用者識別番号候補が入力された時点で該候補を前記利用者特定情報に対して割り当てる利用者識別番号として決定する請求項20記載の埋め込み符号生成装置。

【請求項22】前記利用者識別番号割り当て手段は、前記結託者の利用者識別番号として誤検出される可能性のより低い複数の利用者識別番号を記憶した記憶手段を有し、該記憶手段に記憶された利用者識別番号の中から前記利用者特定情報に対して割り当てる利用者識別番号を選択して読み出す請求項20記載の埋め込み符号生成装置。

【請求項23】前記結託者番号計算手段は、前記複数の剰余対から前記結託者の利用者識別番号である可能性を有する少なくとも一つの利用者識別番号候補を生成し、該候補の中から前記結託者の利用者識別番号として誤検

6

出される可能性のより低い少なくとも一つの利用者識別番号を選択し、該選択した利用者識別番号を前記結託者の利用者識別番号として決定する請求項5記載の埋め込み符号検出装置。

【請求項24】前記結託者番号計算手段は、前記複数の剰余対から前記結託者の利用者識別番号である可能性を有する複数の利用者識別番号候補をシーケンシャルに生成して、該候補について前記結託者の利用者識別番号として誤検出される可能性の高低を判定し、該可能性が低いと判定した全ての利用者識別番号を前記結託者の利用者識別番号として決定する請求項5記載の埋め込み符号検出装置。

【請求項25】前記結託者番号計算手段は、全ての利用者識別番号に対して、全ての前記剰余対中の剰余に対する前記複数の整数を法とする剰余との間の合同式を満足する個数をそれぞれ求め、この数が所定の閾値以上となる利用者識別番号を前記結託者の利用者識別番号候補として生成する請求項23または24記載の埋め込み符号検出装置。

【請求項26】前記結託者番号計算手段は、前記結託者の利用者識別番号として誤検出される可能性のより低い複数の利用者識別番号を記憶した記憶手段を有し、該記憶手段に記憶された利用者識別番号のうち前記複数の剰余対から生成した前記結託者の利用者識別番号である可能性を有する少なくとも一つの利用者識別番号候補に合致した利用者識別番号を前記結託者の利用者識別番号として決定する請求項5記載の埋め込み符号検出装置。

【請求項27】請求項2に記載の埋め込み符号生成装置によって生成された埋め込み符号を前記コンテンツに透かし情報として埋め込む電子透かし埋め込み装置。

【請求項28】所定のコンテンツに対して利用者識別番号の情報を含む透かし情報を埋め込む電子透かし埋め込み装置において、

シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、

出力された符号語を前記透かし情報として前記埋め込み対象コンテンツに埋め込む手段とを具備する電子透かし埋め込み装置。

【請求項29】所定のコンテンツから利用者識別番号の情報を含む透かし情報を検出する電子透かし検出装置において、

シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、

出力された符号語と前記コンテンツとの相関値を求める手段と、

前記相関値に基づいて前記コンテンツ中の前記入力された利用者識別番号に対応する符号語の有無を判定する手段とを具備する電子透かし検出装置。

【請求項30】所定のコンテンツから利用者識別番号の
情報を含む透かし情報を検出する電子透かし検出装置に
おいて、

予め登録された複数の利用者識別番号にそれぞれ対応す
る、シンプレックス符号を構成する複数の符号語を出力
する手段と、

出力された各符号語と前記コンテンツとの各相関値を求
める手段と、

求められた各相関値をベクトルとみなして計算されたノ
ルムに基づいて前記コンテンツ中の透かし情報の有無を
判定し、透かし情報があると判定した場合に前記相関値
に基づいて結託者を特定する手段とを具備する電子透かし
検出装置。

【請求項31】請求項2に記載の埋め込み符号生成装置
によって生成された埋め込み符号が透かし情報として埋
め込まれたコンテンツを格納した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタルデータ
化された音声、音楽、動画、静止画等のコンテンツに対
して透かし情報を埋め込む電子透かし埋め込み装置及び
埋め込み済コンテンツから透かし情報を検出する電子透
かし検出装置に関する。

【0002】

【従来の技術】電子透かし(digital watermarking)は、
デジタルデータ化された音声、音楽、動画、静止画等
のコンテンツに対して、コンテンツの著作権者や利用者の
識別情報、著作権者の権利情報、コンテンツの利用条
件、その利用時に必要な秘密情報、コピー制御情報な
どの情報(これらを透かし情報と呼ぶ)を知覚が容易では
ない状態となるように埋め込み、後に必要に応じて透かし
情報をコンテンツから検出することによって利用制御、
コピー制御を含む著作権保護を行ったり、二次利用の促
進を行うための技術である。

【0003】[電子透かしの要件] 不正利用の防止を目的
とする場合、電子透かし技術はデジタル著作物に対し
て通常に施されると想定される各種の操作や意図的な攻
撃によって、透かし情報が消失したり改竄されたりしな
いような性質(ロバスト性)を持つ必要がある。例えば、
静止画や動画はそれぞれJ P E G (Joint Photographic
Coding Experts Group) 符号化、M P E G (Moving Pictu
re Experts Group) 符号化と呼ばれる非可逆圧縮を施さ
れることが多いため、電子透かし技術はこれらの非可逆
圧縮に対するロバスト性を持つことが重要な要件となる
ことが通常である。

【0004】[電子透かしの分類] 従来、画像に対する電
子透かしの方式は、画素領域利用型と周波数領域利用型
に大別することができる。画素領域利用型の電子透かし
方式は、画素値を変更することで直接的に透かし情報の
埋め込みを行うものである。一方、周波数領域利用型の

電子透かし方式は、直交変換によって、一旦、画素領域
から周波数領域へ移り、周波数領域において埋め込みを
行った後、再び、逆直交変換によって周波数領域から画
素領域に戻るものである。透かし情報は波として埋め込
まれることになる。

【0005】[周波数領域利用型電子透かし方式] 周波数
領域利用型の電子透かし方式としては、例えば文献[1]
Cox, I. J., Kilian, J., Leighton, T. and Shamoon,
T., "Secure Spread Spectrum Watermarking for Mult
imedia", NEC Research Institute, Technical Report
95-10, 1995. (Coxらの方式という)がある。この方式で
は、埋め込み対象となる周波数成分を非可逆圧縮による
影響が小さな低周波数から中間周波数に設定することで
非可逆圧縮に対するロバスト性を実現している。

【0006】[スペクトラム拡散による電子透かし] スペ
クトラム拡散(spread spectrum)の考えを適用すること
で非可逆圧縮へのロバスト性を高める方式がある。スペ
クトラム拡散とは、通信したい信号に必要な帯域に比べ
て十分大きな帯域中に、情報を広く分散させて伝送する
通信方式をいう(文献[2] 山内雪路, "スペクトラム拡
散通信", 東京電機大学出版局, 1994.)。伝送路上のノ
イズに対する耐性が優れている。元のコンテンツを搬送
波、透かし情報を希望波、非可逆圧縮による影響を干渉
波(ノイズ)とみなすことで、スペクトラム拡散の考えを
電子透かし技術へ適用する。スペクトラム拡散による電
子透かし方式として、周波数領域における拡散(先の文
献[1] 参照)が提案されている。

【0007】[周波数領域における拡散(摂動法)] 先の文
献[1]の方式では、透かし情報の埋め込みは画素値に対
して直交変換を行い、周波数領域において透かし情報を
拡散して埋め込む。拡散は、周波数領域において複数の
周波数成分の値とある乱数列に従って変化させることに
よって行う。拡散後、逆直交変換を行う。透かし情報の
検出は、画素値に対して直交変換を行い、埋め込みが行
われた周波数成分の値を埋め込みに用いられた乱数列の
間の相関値によって判定を行う。埋め込まれた透かし情
報は、画素領域では、画像(ブロック)全体に分散されて
いるため、各種の操作に対してロバストである。また、
透かし情報を埋め込んだ周波数成分が低中間周波数領域
にあるならば、低周波数通過フィルタによっても透かし
情報が失われにくい。

【0008】[フィンガープリンティング] 電子透かし方
式において、コンテンツに透かし情報として利用者ID
(利用者識別番号)を埋め込むことで、そのコンテンツの
利用者を特定する情報を埋め込む応用形態が考えられ
る。このような応用形態は「フィンガープリンティン
グ」と呼ばれ、不法コピーいわゆる海賊版の再配布を抑
止する効果が期待できる。

【0009】[結託攻撃問題] ところが、同じコンテンツ
に異なる透かし情報が埋め込まれた複数の埋め込み済

コンテンツが存在する場合、それら複数の埋め込み済コンテンツを利用して透かし情報を改竄、消失させるという行為が考えられる。このような行為は、「結託攻撃(collusion attack)」と呼ばれている。結託攻撃では、複数の埋め込み済みコンテンツの画素値を平均化することで新たなコンテンツを偽造したり、値が異なる画素値や周波数成分値の部分に対して、ランダムに、あるいは、多数決/少数決に従って値を変更する、などのやり方で改変を加える。

【0010】[結託攻撃に対する従来の対策] 従来、結託攻撃に対処する方法として、スペクトラム拡散による方法(先の文献[1]、及び文献[3]山本哲也、渡辺創、嵩忠雄、“すべての結託ユーザを特定可能な電子透かし法”, SCIS'98, 10.2.B, 1998.)と、符号理論的な方法(文献[4] Boneh, Dan and Shaw, James, “Collusion-Secure Fingerprinting for Digital Data”, CRYPTO'95, 452-465, 1995., 文献[5]鈴置昌宏、渡辺創、嵩忠雄, “結託攻撃に強い電子透かし法”, SCIS'97, 31B, 1997. 及び文献[6] 吉田淳、岩村恵市、今井秀樹, “画質劣化が少なく結託攻撃に強い電子透かし法”, SCIS'98, 10.2.A, 1998.)が提案されている。

【0011】文献[1]の方法によれば、利用者毎に $N(0, 1)$ に従う相異なる実乱数列が与えられる。2つの異なる実乱数列の間に相関がないとする。結託攻撃は、画素値を平均化する操作とする。結託によって、検出時の相関値は減衰してしまう。

【0012】文献[1]では、相関値の代わりに、定義された類似度によって結託の検出を行う。この類似度は、相関値を検出された透かし情報のノルムで除したものと定義される。結託により電子透かしのノルムも減衰しているため、相関値が減衰しても類似度はさほど減衰しない。これにより結託者全員を特定することができる。ただし、この方法は検出において埋め込み対象であった原画像を必要とし、また結託者特定に時間がかかるのが難点である。

【0013】文献[3]では、むしろ平均化による結託攻撃の際の相関値の減衰という性質を利用した結託者の特定方法を提案している。結託者間で共通の電子透かしは減衰せず、それ以外の電子透かしは減衰するので、埋め込み時のレベルを保っている電子透かしの組から結託者の組を特定する。全利用者数を n 、想定する最大の結託者数を c とすると、 $(c+1)(c-1)\log_{c+1}n$ オーダの長さの埋め込み符号で結託者を特定することができる。ただし、この方法はスペクトラム拡散法に特有の性質を利用するため、すべての電子透かし方式に適用が可能なわけではない。

【0014】先の文献[4]には、透かし情報を表現する符号において、すべての結託者の間で共通な値を持つビットは検出不能であるという性質を利用して、検出不能なビットがそのまま残るならば、それ以外のビットを如

何に変更しようとも、結託者以外の利用者の符号を生成することができない符号(c-frameproof符号と呼ばれる)を埋め込み符号として生成し、コンテンツに透かし情報として埋め込む方式が提案されている。

【0015】この方式では、埋め込み符号として誰のものでもない符号が生成される可能性は残るものの、ある利用者が自らのコンテンツをそのまま再配布した場合(native redistribution)、その利用者は他者の結託によるものであると主張しての否認はできなくなる。

【0016】結託者の総数に制限が無い n -frameproof符号は、符号サイズが n となる。結託者総数が最大 c である c -frameproof符号は、符号サイズが $16c^2 \log n$ (c は結託者数、 n は全利用者数)である。

【0017】文献[4]ではさらに、2組の結託者のグループがあって、共通部分が空集合の場合、それぞれのグループ内での結託によって生成できる符号(feasible set)の集合間の共通部分も空集合であるような符号(totally c -secure符号)は存在しないことを示している。つまり、結託攻撃によって誰のものでもない符号を生成することができない符号は、厳密には存在しないことを示した。

【0018】そこで、文献[4]では結託者数が c 人以内の場合に結託者を誤って指摘する確率が ϵ 以下である符号(c -secure code with ϵ -error)を埋め込み符号として構成した。まず、誤り ϵ を持つ n -secure符号 $\Gamma(n, 2n^2 \log(2n/\epsilon))$ を構成した。その符号サイズは、 $2n^2(n-1) \log(2n/\epsilon)$ である。

【0019】さらに、それをTraitor Tracingスキーム(文献[7]Chor, B., Fiat, A. and Naor, M., “Tracing traitors”, Proceedings of CRYPTO'94, 257-270, 1994.)と組合せて誤りが ϵ 以下の c -secure符号の可能性を示した。この符号の符号サイズは、 $O(c^4 \log(n/\epsilon) \log(1/\epsilon))$ である。

【0020】[Chernoffの限界(Chernoff bound)] 文献[7]では、Traitor Tracingスキームにおいて、Chernoffの限界の式を利用して結託者を特定するために必要な利用者固有鍵の数を決定している。先の文献[4]では、その方法を流用して誤り ϵ の n -secure符号や c -secure符号を構成した。平均値 p の独立な n 個の確率変数 $X_i \in \{0, 1\}$ があるとき、これらの和が平均値からずれる確率の限界を与えるのがChernoffの限界である。上端と下端の限界は、それぞれ次式で与えられる。

【0021】

【数5】

$$\Pr\left[\sum_{i=1}^n X_i - np > n\delta\right] < \{\exp(\delta/p)/(1+\delta/p)\}^{1-\delta/p} n^p$$

$$\Pr\left[\sum_{i=1}^n X_i - np < -n\delta\right] < \{\exp(-\delta/p)/(1-\delta/p)\}^{1-\delta/p} n^p$$

【0022】さらに、緩い限界として次式が成り立つ。

【0023】

【数6】

$$\Pr\left\{\sum_{i=1}^n X_i - np > n\delta\right\} < 2 \cdot \exp\{-\delta^2 n / (2p(1-p))\}$$

【0024】ここで、 $0 \leq \delta < p(1-p)$ とする。また、次式が成り立つ。

【0025】

【数7】

$$\Pr\left\{\sum_{i=1}^n X_i - np < -n\delta\right\} < \exp\{-\delta^2 n / (2p^2)\}$$

【0026】[結託者中の2人のみを指摘する方法] 文献[4]で提案されている誤り ε のn-secure符号やc-secure符号は、できるだけ多数の結託者を指摘するように設計されていた。利用者を順序集合とみなし、先の文献[4]で示されている $\Gamma_0(n, d)$ 符号を、結託者の集合の中から最大と最小の2人を特定する符号として利用することもできる。この場合には、より小さな符号サイズで $\Gamma_0(n, d)$ 符号を構成することが可能である。

【0027】ここで、 $\Gamma_0(n, d)$ 符号とはdビットを一単位とする連続した1の列及び0の列で構成される符号であり、このようなdビットの1の列や0の列を符号数nに応じた単位数だけ並べて構成される。従って、この符号では1と0はそれぞれdビットを単位として連続するように配置され、dビット未満の数の1や0が孤立して存在することはない。

【0028】例えば、 $d=3$ 、 $n=5$ とすれば、 $\Gamma_0(n, d)$ 符号である $\Gamma_0(5, 3)$ 符号は以下のようになる。

```
1 1 1   1 1 1   1 1 1   1 1 1
0 0 0   1 1 1   1 1 1   1 1 1
0 0 0   0 0 0   1 1 1   1 1 1
0 0 0   0 0 0   0 0 0   1 1 1
0 0 0   0 0 0   0 0 0   0 0 0
```

文献[5]では、2つの符号を昇順と降順に重ね合わせた符号を利用し、結託者中の2人を特定するn-secure符号を提案している。この符号の符号サイズは、 $2n \log_4(2/\varepsilon) = n \log_2(2/\varepsilon)$ となる。文献[6]では、 $\Gamma_0(n, d)$ 符号において $0 < \text{weight}(x | B_S)$ となる最小の $S(S_{\min})$ と、 $\text{weight}(x | B_S) < d$ となる最大の $S(S_{\max})$ を求め、 S_{\min} と $S_{\max}+1$ を結託者であると指摘するアルゴリズムによって結託者の2人を特定する方法を示した。この符号の場合、誤り ε のn-secure符号は、符号サイズが $(n-1) \log_2(2/\varepsilon)$ となる。

【0029】[誤り ε の2-secure符号] 結託者総数が小さな場合には、埋め込み符号の符号サイズを小さくすることが可能である。先の文献[6]には、結託者総数2人の場合に結託者の両方を指摘する符号であって、その符号サイズが $(3n^{1/2}-1) \log_2(6/\varepsilon)$ の埋め込み符号を

示している。

【0030】[結託攻撃耐性の限界] 文献[9] Ergun, Funde, Joe Kilian and Ravi Kumar, "A Note on the Limits of Collusion-Resistant Watermarking", EUROCR YPT'99, 140-149, 1999.)は、電子透かし方式の詳細に依存せずに、結託攻撃に対する耐性には限界があることを理論的に示した。その主張は、正しい結託者を指摘する確率を高くしようとする、誤った利用者を結託者として指摘してしまう確率(偽陽性率)が高くなってしまいうというものであった。

【0031】文献[9]で想定している結託攻撃は、図38に示すように異なるすかし情報が埋め込まれた複数のコンテンツ(コンテンツ1, コンテンツ2, コンテンツ3)を平均化し、その後、ランダムな擾乱を加えるというものである。Ergun等の観点から、例えば先の文献[4]での議論を捉えなおしてみる。文献[4]における議論では、確率論的なc-secure符号の構成要素として $\Gamma_0(n, d)$ 符号を用いている。この $\Gamma_0(n, d)$ 符号は、図39($d=3$ の例)のように(1, 1, 1)と(-1, -1, -1)に符号をとる符号化をn重に直積して得られる。

【0032】この $\Gamma_0(n, d)$ 符号に対して、文献[9]で想定された結託攻撃を適用すると、平均化によって得られるコンテンツは、(1, 1, 1)と(-1, -1, -1)を結ぶ直線上にある重心に移る。結託攻撃は、さらに、その重心からずれた位置にコンテンツを移す。この場合、結託攻撃後のコンテンツが(1, 1, 1)か(-1, -1, -1)の近傍にある場合には、これは結託攻撃によって変更されていないと判断し、原点付近にある場合には結託攻撃によって変更されたとみなすことになる。

【0033】この $\Gamma_0(n, d)$ 符号において、結託者のうち(1, 1, 1)の符号を持つ者の数と(-1, -1, -1)の符号を持つ者の数の間に大きな偏りがある場合、平均化の結果、重心は(1, 1, 1)あるいは(-1, -1, -1)のかなり近くに位置することとなる。その後、ランダムな擾乱を受けるので、一般に、結託者を特定するアルゴリズムは、コンテンツが(1, 1, 1)または(-1, -1, -1)から擾乱によって移ったものか、重心から擾乱によって移ったものかを誤って判断する可能性が高い。つまり、Ergun等自身、彼らの結論がほとんどの電子透かしアルゴリズムに適用されると言明しているが、Boneh等の符号化もErgun等の限界を逃れることはできないといえる。

【0034】一方、 $\Gamma_0(n, d)$ 符号において、2つの符号間の最大距離はnd、最小距離はdと幅が大きい(図40参照)。 $\Gamma_0(n, d)$ 符号は結託攻撃への耐性に重点がおかれていることから、受信空間中に非常にスパースに符号語が配置されているためである。

【0035】電子透かしアルゴリズムは、コンテンツの品質への影響がないように、符号間の最大距離ndの符号を埋め込む必要がある。電子透かしアルゴリズムが、 $\Gamma_0(n, d)$ 符号をコンテンツ空間へ埋め込み、その埋

13

め込みが、符号間の距離とコンテンツ間の距離とが比例するような性質を持つ場合、オリジナルのコンテンツと透かし情報を埋め込んだ後のコンテンツとの間の最大距離も $nd/2$ 以上となるので、 nd が大きな場合には、コンテンツ品質への影響が大きくなる(図41の埋め込み1)。

【0036】仮に、これを避けるため、電子透かしアルゴリズムが符号をコンテンツ空間中のオリジナルコンテンツからの距離関係が保たれないような埋め込みによって、すべての符号語がオリジナルコンテンツとほぼ等しい距離にあるようにしたとすると、 $\Gamma_0(n, d)$ 符号がもともと持っていた結託攻撃への耐性の根拠が失われてしまうことになる(図41の埋め込み2)。

【0037】つまり、Ergun等の限界を意識した上で、結託攻撃に対する耐性の高さとコンテンツの品質への影響の小ささを適切に両立させた符号化による電子透かし方式を実現することが望ましいと考えられる。

【0038】(スペクトラム拡散による電子透かしの結託攻撃耐性) 一方、スペクトラム拡散による電子透かし方式では、埋め込みの影響がコンテンツ品質に大きな影響を与えないように埋め込み強度が設定される。その上で、埋め込みに用いる擬似乱数列が符号語に対応する。

【0039】標本値空間と周波数空間の間の直交変換は線形写像なので、攻撃対象の電子透かし方式が空間領域利用型であれ周波数領域利用型であれ、Ergun等の結託攻撃は擬似乱数列を平均化して、さらに擾乱を与えるという操作となる。

【0040】スペクトラム拡散による電子透かし方式では、符号語である擬似乱数列は相互相関(cross-correlation)がほとんどゼロとなるように選択されることが普通である。従って、 k 個のコンテンツの平均によって得られるコンテンツは、ある結託者に対応する擬似乱数列との相関が $1/k$ に減衰すると考えられる。擬似乱数列間の相互相関が十分小さく、かつ、この k があまり大きくなければ、電子透かしの検出において相関値があるあらかじめ定められた閾値を越えるため、結託者を特定することが可能である。

【0041】前述した文献[1]の方式は、検出においてオリジナルコンテンツを利用することを前提としており、相関値の代わりに類似度(similarity)と呼ばれる量を用いて検出が行われる。類似度は、検出対象コンテンツからオリジナルコンテンツを引いた差分と埋め込みに用いた擬似乱数列の間の相互相関値を差分の自己相関値の平方根で正規化したものである。

【0042】類似度による検出では、結託攻撃における平均化によって、分子の相関値が $1/k$ に減衰するが、分母の差分のノルムも $1/k$ に減衰するため、類似度は減衰しないことが期待される。ただし、平均化以外にノイズが加わる場合には、そのノイズの影響は正規化によってかえって大きくなる。

14

【0043】文献[10] Kilian, Joe, F. Thomas Leighton, Lesley R. Matheson, Talal G. Shamooun, Robert E. Tarjan, and Francis Zane, "Resistance of Digital Watermarks to Collusive Attacks", Technical Report TR-585-98, Department of Computer Science, Princeton University, 1998. では、統計的な議論によって文献[1]の電子透かし方式が何人までの結託者による結託攻撃に対する耐性を持っているかという理論的考察を行っている。疑似乱数系列はガウシアンノイズを仮定し、結託攻撃は結託者の持つコンテンツからオリジナルコンテンツを統計的に推定することで行うと仮定する。その結果、現実的なパラメータ設定で、数名から十数名の結託者に対する耐性を実現することが可能であるという結論が得られている。

【0044】また、電子透かしの応用形態によっては、オリジナルコンテンツを用いた検出が行えず、検出対象コンテンツのみから検出を行う必要がある場合がある。その場合には、類似度による検出は行えない。この場合には、許容される結託者の数はさらに小さくなると考えられる。

【0045】ところで、文献[1]や文献[10]での議論は、すべて、符号語である擬似乱数列の間の相互相関が十分小さいという前提に基づいている。しかし、一般に擬似乱数列の数が増えてくると、仮にそれをランダムに選択したとしても、偶然に大きな相互相関値を持つ対が生ずる可能性が高くなってくると思われる。

【0046】いったい、どの程度多くの擬似乱数系列が任意の対の間で相互相関値を小さくできるのか、また、そのような性質を持つ擬似乱数列をどのように選択すれば良いのか、そして、そのようにして選択された擬似乱数列を符号語として、どのような電子透かし方式を実現すれば、結託攻撃に強い方式となるのが未解決の問題として残されている。

【0047】この問題も、先に[結託攻撃耐性]の項で述べた文献[9]での限界を意識した上で、結託攻撃に対する耐性の高さとコンテンツの品質への影響の小ささを適切に両立させた符号化による電子透かし方式をどう実現させるかという問題の一つと考えられる。

【0048】相互相関の小さな2値の擬似ランダムビット列を生成する方法として、M系列を利用する方法が知られている。M系列は、線形フィードバックシフトレジスタ(LFSR)の出力として得られる系列のうち、LFSRがGF(2)の原始多項式の係数に対応するタップを持つ場合に生成されるものである。M系列中の1と0をそれぞれ+1と-1に置き換えると、PN系列となる。M系列は、0の出現頻度が1の出現頻度がほぼ等しく(1の出現頻度が一回少ない)、その間の相互相関関数は0のとき値1、0以外のとき $-1/L$ となる。ここで、 L は系列の周期で、レジスタの段数を n とすると、 $L = 2^n - 1$ である。

15

【0049】M系列から得られたPN系列を巡回シフトして得られる系列を符号語として採用すれば、相互相関の小さな符号語が得られる。これらの符号語を電子透かしの埋め込みの際の擬似乱数系列として用いれば良い。この乱数系列は、空間領域利用型と周波数領域利用型の両方のスペクトラム拡散による電子透かしに利用できる。

【0050】周波数領域利用型のスペクトラム拡散の電子透かし方式では、普通、 $N(0, 1)$ に従うガウシアンノイズを符号語とする。相互相関が小さな符号語を複数構成するには、逐次乱数列を生成し、それが、それまでに生成したすべての乱数列との相関が小さいことを確認し、仮に、大きな相互相関値を持つ場合には、その乱数列は符号語として採用しないという方法をとる。

【0051】しかし、この方法では、新たに生成した乱数列がそれまでに生成した乱数列と小さな相互相関であるという保証がないため、せっかく生成した乱数列を捨てなければならないことがあるため処理が無駄である。特に、乱数列の数がある程度以上増えると、その確率は高くなる。

【0052】

【発明が解決しようとする課題】以上に説明したように、従来の電子透かし技術では、結託攻撃によって透かし情報が失われたり偽造されたりすることで、不正な再配布が行われても、その不正行為者を特定できなくなる恐れがあった。

【0053】また、結託攻撃へのロバスト性を実現する従来の提案において、非常に冗長な形で透かし情報を埋め込む必要があるため、あまり大きな利用者総数や結託者数を想定することができないという欠点があった。大きな利用者総数及び結託者数を想定しても大きな符号サイズの埋め込み符号を透かし情報として埋め込むことは、コンテンツの品質劣化を招く原因となる。

【0054】さらに、結託者特定の際の埋め込み符号の検出誤りを正しく評価した上で透かし情報(埋め込み符号)を構成する必要があるが、従来の電子透かし技術ではこのような点に対する考察、特に3人以上の結託者が改竄に関与した場合の対策が不十分であり、また検出誤りに対して必要以上に透かし情報である埋め込み符号の符号サイズを大きくしてしまう可能性があった。

【0055】本発明の目的は、結託攻撃への耐性を有し、利用者総数や結託者総数が大きな場合においても、コンテンツの品質劣化を極力抑えて透かし情報を埋め込む電子透かし埋め込み装置及び電子透かし検出装置と、これらに用いられる埋め込み符号生成方法及び装置、埋め込み符号検出方法及び装置を提供することにある。

【0056】本発明の他の目的は、結託攻撃への耐性を有し、かつ3人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成する埋め込み符号生成装置及びその

16

埋め込み符号を正しく検出して復号する埋め込み符号検出方法及び装置を提供することにある。

【0057】

【課題を解決するための手段】上記の課題を解決するため、本発明に係る第1の埋め込み符号生成装置は、所定のコンテンツに埋め込まれるべき埋め込み符号を生成する埋め込み符号生成装置において、前記コンテンツを利用する利用者の利用者識別番号に対して、互いに素の関係にある複数の整数を法とする複数の剰余を計算する剰余計算手段と、前記剰余計算手段により求められた各剰余を表す複数の成分符号(例えば、所定のビット数を一単位とする連続した1の列及び0の列で構成される符号)を生成する成分符号生成手段と、前記成分符号生成手段により生成された各成分符号を接続して前記埋め込み符号を生成する接続手段とを具備することを特徴とする。

【0058】この第1の埋め込み符号生成装置においては、前記利用者識別番号の割り当て要求に対して、複数の利用者識別番号候補の中から前記結託者の利用者識別番号として誤検出される可能性のより低い一つの候補を選択し、該選択した利用者識別番号を前記利用者特定する利用者特定情報に対して割り当てる利用者識別番号割り当て手段をさらに具備してもよい。

【0059】前記利用者識別番号割り当て手段は、第1の態様によると前記複数の利用者識別番号候補を一つずつシーケンシャルに入力して、該候補について前記結託者の利用者識別番号として誤検出される可能性の高低を判定し、該可能性が低いと判定した利用者識別番号候補が入力された時点で該候補を前記利用者特定情報に対して割り当てる利用者識別番号として決定する特徴とする。

【0060】請求項20記載の埋め込み符号生成装置。

【0061】第2の態様による前記利用者識別番号割り当て手段は、前記結託者の利用者識別番号として誤検出される可能性のより低い複数の利用者識別番号を記憶した記憶手段を有し、該記憶手段に記憶された利用者識別番号の中から前記利用者特定情報に対して割り当てる利用者識別番号を選択して読み出すことを特徴とする。

【0062】第1の埋め込み符号生成装置に対応する本発明に係る第1の埋め込み符号検出装置は、所定のコンテンツに埋め込まれた複数の成分符号を接続した埋め込み符号を検出する埋め込み符号検出装置において、前記埋め込み符号を前記複数の成分符号に分割する符号分割手段と、分割された各成分符号をそれぞれ復号して予め定められた互いに素の関係にある複数の整数を法とする2つの剰余からなる複数の剰余対を得る成分符号復号手段と、前記複数の剰余対から前記コンテンツに対して結託攻撃を行った結託者の利用者識別番号を計算する結託者番号計算手段とを具備することを特徴とする。また、複数の剰余対から結託の有無を判定する結託有無判定手

17

段をさらに有し、この結託判定手段により結託があると判定されたとき、結託者番号計算手段が結託者の利用者識別番号を計算するようにしてもよい。

【0063】ここで、前記結託者番号計算手段は、第1の態様によると、入力された k' 個の剰余対の各々から一方の剰余を選択して k' 個の剰余の組($R_1, R_2, \dots, R_{k'}$)を生成する剰余選択部と、前記剰余選択部により生成された k' 個の剰余の組から選択された異なる k 個の剰余(S_1, S_2, \dots, S_k)から中国剰余定理に従って結託者の利用者識別番号 u の候補を計算する中国剰余定理部と、前記剰余選択部により生成された k' 個の剰余の組から前記 k 個の剰余を選択して前記中国剰余定理部に渡し、前記中国剰余定理部により計算された結託者の利用者識別番号候補 u の候補から該結託者の利用者識別番号を特定して出力する一貫性検査部とを含み、前記一貫性検査部は、前記剰余選択部により生成された k' 個の剰余の組から前記 k 個の剰余を選択する選択処理と、前記中国剰余定理部により計算された結託者の利用者識別番号 u の候補と残りの $(k' - k)$ 個の剰余のうちの所定個数(y)の剰余との間に $R_i = u \bmod p_i$ ($i = 1, 2, \dots, i_z$)の関係が成立するかどうかを判定する判定処理と、該判定処理により前記関係が成立する場合に結託者の利用者識別番号として出力する出力処理とを有し、前記関係が成立しない場合には前記剰余選択部により生成された k' 個の剰余の組から前記選択処理により新たな組み合わせの k 個の剰余(S_1, S_2, \dots, S_k)を選択して前記判定処理を行い、全ての組み合わせの k 個の剰余(S_1, S_2, \dots, S_k)に対して前記関係が成立しない場合には前記剰余選択部に対して新たな k' 個の剰余の組を要求して、前記関係が成立するまで前記選択処理及び判定処理を繰り返すことを特徴とする。

【0064】第2の態様による前記結託者番号計算手段は、前記複数の剰余対から前記結託者の利用者識別番号である可能性を有する少なくとも一つの利用者識別番号候補を生成し、該候補の中から前記結託者の利用者識別番号として誤検出される可能性のより低い少なくとも一つの利用者識別番号を選択し、該選択した利用者識別番号を前記結託者の利用者識別番号として決定することを特徴とする。

【0065】第3の態様による前記結託者番号計算手段*

$$\left[1 - \prod_{i=1}^z \left\{ 1 - \left(1 - \frac{1}{p_i} \right)^c \right\} \right]^{d(n) \cdot C(n) \cdot 2^{n-1}} \geq 1 - \frac{\varepsilon}{2} \quad (1)$$

【0067】の条件を満たすように設定されていることを特徴とする。

【0068】ここで、前記計算手段は、例えば入力された利用者識別番号に対応して互いに素の関係にある複数の

18

*は、前記複数の剰余対から前記結託者の利用者識別番号である可能性を有する複数の利用者識別番号候補をシーケンシャルに生成して、該候補について前記結託者の利用者識別番号として誤検出される可能性の高低を判定し、該可能性が低いと判定した全ての利用者識別番号を前記結託者の利用者識別番号として決定することを特徴とする

また、第2及び第3の態様による前記結託者番号計算手段において、全ての利用者識別番号に対して、全ての前記剰余対中の剰余に対する前記複数の整数を法とする剰余との間の合同式を満足する個数をそれぞれ求め、この数が所定の閾値以上となる利用者識別番号を前記結託者の利用者識別番号候補として生成することを特徴とする

第4の態様による前記結託者番号計算手段は、前記結託者の利用者識別番号として誤検出される可能性のより低い複数の利用者識別番号を記憶した記憶手段を有し、該記憶手段に記憶された利用者識別番号のうち前記複数の剰余対から生成した前記結託者の利用者識別番号である可能性を有する少なくとも一つの利用者識別番号候補に合致した利用者識別番号を前記結託者の利用者識別番号として決定することを特徴とする

本発明に係る第2の埋め込み符号生成装置は、入力された利用者識別番号に対応して複数の整数要素の組を計算する計算手段と、所定個数の利用者識別番号に対して前記計算手段により計算される全ての整数要素の組を表現可能な k' 個の成分符号のうちの k 個の組み合わせが前記利用者識別番号を一意に表現できる成分符号を前記各整数要素に対応してそれぞれ生成する成分符号生成手段と、この成分符号生成手段により生成された各成分符号を接続して埋め込み符号を生成する接続手段とを具備し、前記 k' は、3以上の正整数を c 、1以上の正整数を z 、前記埋め込み符号の検出時に前記各成分符号から検出できる前記整数要素の個数を q として、 $c(k+z)/q$ 以上となるように決定されていることを特徴とし、より好ましくは前記所定個数の利用者識別番号に対して前記計算手段により計算される各整数要素のとり得る値を p_i ($i = 1, 2, \dots, k'$)とし、前記埋め込み符号の検出時に想定される検出誤り率を ε としたとき、前記 k' は、

【0066】

【数8】

の整数を法とする剰余の組を前記整数要素の組として計算するか、あるいは入力された利用者識別番号に対応して平行移動によって定義される同値類に属する要素の番号の組を前記整数要素の組として計算する。後者の場

19

合、式(1)の条件に加え、前記 p_i ($i=1, 2, \dots, k'$)を同一の正整数 p として、

$$k' = \frac{c}{2}(k+z) \leq \frac{p^t - 1}{p - 1}$$

【0070】の条件をさらに満たすことを特徴とする。

【0071】第2の埋め込み符号生成装置に対応する本発明に係る第2の埋め込み符号検出装置は、所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能な k' 個の成分符号のうちの k 個の組み合わせが利用者識別番号を一意に表現できる成分符号であって、入力された利用者識別番号に対応して計算された整数要素の組に対応して生成された部分を接続した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、抽出された各成分符号に分割する符号分割手段と、分割された各成分符号をそれぞれ復号する成分符号復号手段と、各成分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、前記 k' は、3以上の正整数を c 、1以上の正整数を z 、前記埋め込み符号の検出時に前記各成分符号から検出できる前記整数要素の個数を q として、 $c(k+z)/q$ 以上となるように決定されていることを特徴とし、より好ましくは前記所定個数の利用者識別番号に対して計算される各整数要素のとりうる値を p_i ($i=1, 2, \dots, k'$)とし、前記埋め込み符号の検出時に想定される検出誤り率を ε としたとき、前記 k' は、式(1)の条件を満たすように設定されていることを特徴とする。

【0072】ここで、前記整数要素の組は、例えば前記利用者識別番号に対応して計算された互いに素の関係にある複数の整数を法とする剰余の組、あるいは前記利用者識別番号に対応して計算された平行移動によって定義される同値類に属する要素の番号の組であり、後者の場合、式(1)の条件に加え、前記 p_i ($i=1, 2, \dots, k'$)を同一の正整数 p として、式(2)の条件をさらに満たすことを特徴とする。

【0073】本発明に係る第3の埋め込み符号検出装置は、所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能な k' 個の成分符号のうちの k 個の組み合わせが利用者識別番号を一意に表現できる成分符号であって、入力された利用者識別番号に対応して計算された整数要素の組に対応して生成された部分を接続した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、抽出された各成分符号に分割する符号分割手段と、分割された各成分符号をそれぞれ復号する成分符号復号手段と、各成分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、前記成分符号復号手段は、前記各成分符号をブロックに分割するブロック分割部と、該ブロック毎にブロック内の“1”のビット数を計数する

20

*【0069】

【数9】

(2)

計数部と、該計数部で得られた計数値が第1の閾値を越えているか否かを判定する第1の判定部と、前記計数値が第2の閾値に満たないか否かを判定する第2の判定部と、前記第1の判定部で第1の閾値を越えていると判定された最小のブロックを決定する最小位置決定部と、前記第2の判定部で第2の閾値に満たないと判定された最大のブロックを決定する最大位置決定部とを有し、前記最小位置決定部及び最大位置決定部の決定結果を復号結果として出力することを特徴とする。

【0074】さらに、本発明によると上述した第1または第2の埋め込み符号生成装置によって生成された埋め込み符号を埋め込み対象コンテンツに透かし情報として埋め込む電子透かし埋め込み装置が提供される。

【0075】本発明に係る他の電子透かし埋め込み装置は、埋め込み対象コンテンツに対して利用者識別番号の情報を含む透かし情報を埋め込む電子透かし埋め込み装置であって、シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、出力された符号語を透かし情報として埋め込み対象コンテンツに埋め込む手段とを具備することを特徴とする。

【0076】本発明に係る他の電子透かし検出装置は、入力されたコンテンツから利用者識別番号の情報を含む透かし情報を検出する電子透かし検出装置であって、シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、出力された符号語とコンテンツとの相関値を求める手段と、この相関値に基づいてコンテンツ中の入力された利用者識別番号に対応する符号語の有無を判定する手段とを具備することを特徴とする。

【0077】このような本発明に基づく埋め込み符号生成装置／埋め込み符号復号装置及び電子透かし埋め込み／検出装置においては、透かし情報である埋め込み符号の符号サイズを大きくすることなく、利用者総数や結託者数が大きくなっても、結託攻撃に対するロバスト性を得ることができる。

【0078】また、 $k' \geq c(k+z)/q$ 以上という条件、さらには式(1)や式(2)の条件を満たすようにすることによって、3人以上の結託者が改竄に関与した場合においても、埋め込み符号検出時の正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成する埋め込み符号生成装置及びその埋め込み符号を正しく復号する埋め込み符号復号装置が実現される。

【0079】

【発明の実施の形態】図1は、本発明の電子透かし埋め

21

込み装置 1 と電子透かし検出装置 2 が適用されるシステムの例であるフィンガープリンティングシステムの概念図を示す。画像や音声などの埋め込み対象コンテンツと利用者識別番号 (以下、利用者識別番号を利用者 ID という) が電子透かし埋め込み装置 1 に入力され、ここで得られた埋め込み済みコンテンツがこれを格納する記憶媒体を含む流通経路 3 を経て流通する。

【0080】前述した結託攻撃は、流通経路 3 において埋め込みコンテンツに対して行われる。このような結託攻撃に対抗するために、本発明に基づく電子透かし検出装置 2 では、結託の有無を示す結託判定信号、結託があった場合の結託者を特定する結託者 ID (結託者の利用者 ID)、及び結託がなかった場合の正規の利用者 ID が生成される。

【0081】以下、本発明による電子透かし埋め込み装置及び電子透かし検出装置の実施形態について説明する。

(第 1 の実施形態) 本発明の第 1 の実施形態として、従来例よりも小さな符号サイズを持つ ε 誤りの c-secure 符号を埋め込み符号とする電子透かし埋め込み装置及び電子透かし検出装置について説明する。図 2 (a) (b) は、本発明の第 1 の実施形態に係る電子透かし埋め込み装置及び電子透かし検出装置の概略構成を示している。図 2 (a) に示す電子透かし埋め込み装置は、埋め込むべき透かし情報である利用者 ID の埋め込み符号を生成する埋め込み符号生成部 11 と、生成された埋め込み符号を埋め込み対象コンテンツに埋め込み、埋め込み済みコンテンツを得る符号埋め込み部 12 とから構成される。一方、図 2 (b) に示す電子透かし検出装置は、検出対象コンテンツ (例えば、埋め込み済みコンテンツ) から埋め込み符号を抽出する埋め込み符号抽出部 13 と、抽出された埋め込み符号を検出して復号する埋め込み符号検出部 14 とから構成される。

【0082】図 3 は、埋め込み符号生成部 11 の構成を示している。この埋め込み符号生成部 11 は、それぞれ k' 個の法記憶部 21-1, 21-2, ..., 21- k' 、剰余計算部 22-1, 22-2, ..., 22- k' 、成分符号生成部 24-1, 24-2, ..., 24- k' と、符号パラメータ記憶部 23 及び符号接続部 25 からなる。

【0083】法記憶部 21-1, 21-2, ..., 21- k' には、互いに素の関係にある整数、この例では相異なる k' 個の素数 $p_i (i=1, 2, \dots, k')$ が記憶されており、これらの素数 p_i が剰余計算部 22-1, 22-2, ..., 22- k' に法として供給される。剰余計算部 22-1, 22-2, ..., 22- k' は、入力される利用者 ID u に対して、素数 p_i を法とする剰余 $u_i = u \bmod p_i (i=1, 2, \dots, k')$ をそれぞれ求める。すなわち、入力された利用者 ID に対応した複数の整数要素の組として、剰余計算部 22-1, 22-2, ..., 50

22

22- k' により剰余 $u_i = u \bmod p_i (i=1, 2, \dots, k')$ が計算される。

【0084】成分符号生成部 24-1, 24-2, ..., 24- k' は、 k' 個の素数 $p_i (i=1, 2, \dots, k')$ に対して、符号パラメータ記憶部 23 に記憶された符号パラメータ t に従って剰余計算部 22-1, 22-2, ..., 22- k' により求められた剰余 $u_i (i=1, 2, \dots, k')$ を表す前述した $\Gamma_0(n, d)$ 符号からなる成分符号 $\Gamma_0(p_i, t)$ をそれぞれ生成する。すなわち、成分符号生成部 24-1, 24-2, ..., 24- k' では、所定個数 (n) の利用者 ID に対して剰余計算部 22-1, 22-2, ..., 22- k' で計算される全ての剰余 $u_i (i=1, 2, \dots, k')$ の組を表現可能な k' 個の成分符号のうちの k 個の組み合わせが利用者 ID を一意に表現できる成分符号 $\Gamma_0(p_i, t)$ を各剰余に対応して生成する。

【0085】符号接続部 25 は、成分符号生成部 24-1, 24-2, ..., 24- k' により生成された各成分符号 $\Gamma_0(p_i, t)$ を接続することによって、透かし情報である埋め込み符号を生成する。

【0086】図 4 に、成分符号生成部 24-1, 24-2, ..., 24- k' の一つ (24- i) の構成を示す。符号パラメータを t 、剰余を u_i 、法を p_i とすると、減算部 31 では $p_i - u_i - 1$ が求められる。“0” 列生成部 32 では、符号パラメータ t と剰余 u_i に基づき $t \times u_i$ ビットの連続した “0” 列が生成され、“1” 列生成部 33 では、符号パラメータ t と減算部 31 からの出力 $p_i - u_i - 1$ に基づき $t \times (p_i - u_i - 1)$ ビットの連続した “1” 列が生成される。そして、これらの “0” 列と “1” 列が接続部 34 で接続され、 $t \times (p_i - 1)$ ビットのビット列が $\Gamma_0(n, d)$ 符号からなる成分符号 $\Gamma_0(p_i, t)$ として生成される。

【0087】図 5 は、こうして生成される成分符号の一例を示している。0 から $n-1$ までの n 個の利用者 ID に対応して、 $B(0), \dots, B(n-2)$ のブロック “0” 列からなる成分符号が割り当てられている。

【0088】図 6 に、図 2 (b) における埋め込み符号検出部 14 の構成を示す。この埋め込み符号検出部 14 は、検出対象コンテンツから図 2 (b) の埋め込み符号抽出部 13 で抽出された埋め込み符号を入力とする符号分割部 41、成分符号復号部 42-1, 42-2, ..., 42- k' 、利用者 ID 計算部 43、結託判定部 44-1, 44-2, ..., 44- k' 、結託判定 OR 部 45 及び結託者 ID 計算部 46 から構成されている。

【0089】検出対象コンテンツから埋め込み符号抽出部 13 により抽出された透かし情報である埋め込み符号は、符号分割部 41 により各成分符号に分割された後、成分符号復号部 42-1, 42-2, ..., 42- k' により復号されることにより、利用者 ID に対応する剰余対が生成される。

23

【0090】こうして生成された各剰余対の一方の剰余から、利用者ID計算部43により利用者IDが計算で求められ、また各剰余対から結託判定部44-1, 44-2, ..., 44-k'により結託の有無が判定される。結託判定部44-1, 44-2, ..., 44-k'の判定結果について、結託判定OR部45で論理和がとられることにより、結託が存在したか否かが最終的に判定される。さらに、結託が存在すると判定されたときは各剰余対から結託者ID計算部46で結託者IDが計算され、結託者が特定される。

【0091】図7に、結託者ID計算部46の詳細な構成を示す。この結託者ID計算部46は、k'個の剰余対から各一つの剰余を選択する剰余選択部51、選択されたk'個の剰余のうちk個の剰余を選択する一貫性検査部52、及び一貫性検査部52で選択されたk個の剰余に対して中国剰余定理を適用して結託者ID候補を得る中国剰余定理部53からなる。

【0092】図8に、図7中の一貫性検査部52の内部構成を示す。中国剰余定理部53により得られた結託者ID候補は一貫性検査部52にフィードバックされ、k'個の剰余のうち残りの(k'-k)個の剰余との間の一貫性検査が行われて、最終的に結託者IDが求められる。図8の一貫性検査部52は、剰余の(k+z)組の生成部521と、剰余のz組と結託者ID候補の一貫性検査部522から構成される。その動作については、後に説明する。

【0093】本実施形態の電子透かし埋め込み装置及び電子透かし検出装置によると、利用者総数や結託者総数が大きい場合においても、コンテンツの品質劣化の少ない電子透かしが可能となる。以下、詳細に説明する。利用者総数をnとし、結託者総数の最大値をcとする。一方、図3の法記憶部21-1, 21-2, ..., 21-k'で用意されているk'個の素数 $p_1, p_2, \dots, p_{k'}$ から任意のk個の素数を選んだとき、それらのk個の素数の積はn以上とする。例えば、この積は $n \leq p_1 \times p_2 \times \dots \times p_k$ である。

【0094】埋め込み符号生成部12では、各素数 p_i ($i=1, 2, \dots, k'$)に対して、図3の成分符号生成部24-1, 24-2, ..., 24-k'により成分符号 $\Gamma_0(p_i, t)$ が生成される。これらの成分符号 $\Gamma_0(p_i, t)$ を符号接続部25により接続することによって、新たな符号 $\Gamma(p_1, p_2, \dots, p_{k'}; n, t)$ が生成される。

【0095】ここで、各利用者の利用者IDをuとすると、その利用者IDuに対応する接続符号 $\Gamma(p_1, p_2, \dots, p_{k'}; n, t)$ の符号語は、各成分符号 $\Gamma_0(p_i, t)$ がその利用者IDuに対する素数 p_i を法とする、剰余計算部22-1, 22-2, ..., 22-k'で計算された剰余 $u \bmod p_i$ を表す符号語となり、これが透かし情報(埋め込み符号)として埋め込み対象コンテンツに埋め

24

込まれることになる。

【0096】このようにして得られた埋め込み済みコンテンツに対して結託攻撃が行われた場合、図6の電子透かし検出装置において、符号分割部41で分割された各成分符号 $\Gamma_0(p_i, t)$ を成分符号復号部42-1, 42-2, ..., 42-k'で復号することによって、c人中のある2人の利用者IDの p_i に関する剰余(residue)の対が得られる。これを p_i に関する剰余対(residue pair)と呼ぶことにする。

【0097】また、 p_i に関する剰余対中のある剰余がある利用者IDuを保有する結託者の剰余であるとき、その剰余は利用者IDuを保有する結託者に起因すると呼ぶことにする。このとき、この結託者を含めて結託者と同じ剰余の値を持つ利用者に関しては、その剰余はその利用者の利用者IDに起因する可能性があると呼ぶことにする。

【0098】(中国剰余定理(Chinese Remainder Theorem)) 相異なるk個の素数 p_1, p_2, \dots, p_k が与えられたとき、各 i ($i=1, 2, \dots, k$)について $u_i \in \mathbb{Z}_{p_i}$ が与えられると、 $u_i \equiv u \bmod p_i$ である $u \in \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \dots \times \mathbb{Z}_{p_k}$ が一意に定まり、帰納的に計算できる。これが中国剰余定理である。

【0099】中国剰余定理を適用すると、図7に示すように中国剰余定理部53にk'個の素数のうちk個の素数に対応する剰余が与えられれば、それから利用者IDを一意に定めることができる。しかし、それらの剰余すべてが同一結託者の利用者IDに起因するとは限らないため、求めた利用者IDが結託者を正しく特定するとは限らない。

【0100】そこで、さらに余分にz個の剰余を用意し、(k+z)個の剰余の間の一貫性を検査することで、得られた利用者IDの正当性を検証する。言い換えると、(k+z)個の連立合同方程式の解の存在を確認する。例えば、k個の剰余から得られた利用者IDに対して、残りの剰余 r_{k+1}, \dots, r_{k+z} に対応する整数 p_{k+1}, \dots, p_{k+z} で除した余り(remainder)を求め、それらがそれぞれ剰余 r_{k+1}, \dots, r_{k+z} に一致し、一致したか否かで結託者を判定することとする。

【0101】すなわち、図7の一貫性検査部52では図8に示すように、図7の剰余選択部51でk'個の剰余対から各一つ選択されたk'=c(k+z)/2個の剰余を剰余の(k+z)組の生成部521に入力し、これらk'個の剰余の中からk個の剰余を選択して中国剰余定理部53に引き渡す。さらに、一貫性検査部522により剰余のz組と結託者ID候補との一貫性検査を行って、結託者ID(結託者の利用者ID)を出力する。

【0102】結託者数が2人の場合については、この方法を比較的容易に実現できる(例えば、特願平10-108039, 特願平10-122108)。ここでは、それを一般の結託者数に拡張する。

25

【0103】利用者総数を n とし、結託者の最大数を c とする。先の文献[13]によって導入された ε 誤りを持つ n -secure符号(cubic length n -secure code with ε -error)は、以下のように定義される。

【0104】(定義1) $((n-1)d, n)$ 符号 $\Gamma_0(n, *$

$$w^{(i)}|_{B_j} = \begin{cases} \{0\}^d & \text{for } i > j \\ \{1\}^d & \text{otherwise} \end{cases} \quad (3)$$

【0106】ここで、 $w^{(i)}|_{B_j}$ は符号語 $w^{(i)}$ をビット位置の集合 B_j に制限したものである。集合 B_i , $i = 0, \dots, n-2$ はブロック(blocks)と呼ばれ、 d 個のビット位置から構成される。異なるブロック間は共通部分を持たない($i \neq j$ に対して $B_i \cap B_j = \emptyset$)。

【0107】すべての利用者に対して、シリアル番号のような形で順序をつけることができると仮定する。 i 番目の利用者に対して、符号語 $w^{(i)}$ を割り当てるとする。さらに、利用者は自分に割り当てられたシリアル番号を知らされていないとする。

【0108】先の文献[12][14]によって導入された ε 誤りを持つ線形 n -secure符号(linear length n -secure code with ε -error)は、符号語は定義1で定義された符号と同一であるが、検出アルゴリズムが異なる。この符号は、結託者中で最大と最小のシリアル番号をもつ2人の結託者を特定することができる。符号サイズは、 $\Theta(n)$ である。

【0109】(定理1) 以下の検出アルゴリズム1を符号 $\Gamma_0(n, d)$ に適用するとする。 $d = \log_2(2/\varepsilon)$ ならば、この符号は ε 誤りを持った n -secure符号である。

【0110】(検出アルゴリズム1)

- (1) 検出された符号 $x \in \{0, 1\}^z$ を入力する。ここで、 $z = (n-1)d$, $d = \log_2(1/\varepsilon)$ とする。
- (2) $s = 0$ から $n-2$ まで、以下を実行する:
(2-1) もし、 $x|_{B_s} \neq \{0\}^d$ ならば中断する。
- (3) $t = n-2$ から S まで、以下を実行する:
(3-1) もし、 $x|_{B_{t-1}} \neq \{0\}^d$ ならば中断する。
- (4) s と t を出力する。

【0111】次に、本発明に特有のアルゴリズム部分について説明する。 k, k', z は、 $k' = c(k+z)/2$ を満足する正整数とする。 $p_1, \dots, p_{k'}$ は、互いに素の関係にある整数とする。 p は $p_1, \dots, p_{k'}$ のうち最小のものとする。また、 $p_1, \dots, p_{k'}$ のうち小さい方から選んだ k 個の積を n 以上とする。これらの整数 $p_1, \dots, p_{k'}$ を以下では因数と呼ぶことにする。

【0112】これらの因数の平均値を p_{ave} とする($p_{ave} = (p_1 + \dots + p_{k'})/k'$)。 $i = 1, \dots, k'$ の各 p_i に対応して、先の文献[13]の n -secure符号 $\Gamma_0(p_i, t)$ を構成要素の符号として用意する。

【0113】(定義2) $((p_{ave}-1)k', t, n)$ 符号 $\Gamma(p_1, \dots, p_{k'}; n, t)$ は、その符号語 $W^{(1)}, \dots, W^{(n)}$ が

26

* d)は、その符号語 $w^{(0)}, \dots, w^{(n-1)}$ が次の条件を満たす符号と定義する。

【0105】

【数10】

次のように構成された符号であると定義する。

$W^{(u)}|_{C_i} = w^{(u \bmod p_i)} \in \Gamma_0(p_i, t)$

ここで、 C_i は構成要素の符号 $\Gamma_0(p_i, t)$ に対応するビット位置の集合である。この符号を u 番目の利用者に割り当てることとする。

【0114】埋め込み符号生成のための符号化アルゴリズムは、次の通りである。

(符号化アルゴリズム)

(1) 利用者ID $u \in \{0, \dots, n-1\}$ を入力する。

(2) $i = 1$ から k' まで以下を実行する:

(2-1) $u \bmod p_i$ を計算し、符号語 $w^{(u \bmod p_i)} \in \Gamma_0(p_i, t)$ を生成する。

(3) 生成された符号語を接続して、一つの符号語 $W^{(u)}$ とする。

この符号化アルゴリズムにより生成された埋め込み符号の検出アルゴリズムとしては、先の検出アルゴリズム1を利用する。

【0115】(定義3) $\Gamma(p_1, \dots, p_{k'}; n, t)$ の構成要素に対して、検出アルゴリズム1を適用することで、高々2つの整数 $r_i^{(-)}, r_i^{(+)} \in \mathbb{Z}_{p_i}$ を得る。ここで、 $0 \leq r_i^{(-)} \leq r_i^{(+)} \leq p_i$ である。これらの整数 $r_i^{(-)}, r_i^{(+)} \in \mathbb{Z}_{p_i}$ を $\Gamma_0(p_i, t)$ の剰余(residues)と呼ぶことにする。また、集合 $\{r_i^{(-)}, r_i^{(+)}\}$ を $\Gamma_0(p_i, t)$ の剰余対(residue pair)と呼ぶことにする。

【0116】(定義4) r を $\Gamma_0(p_i, t)$ の剰余とする。結託者の集合の中に $r \equiv u \bmod p_i$ を満たす結託者が存在する場合、剰余 r は u に起因する(r arises from u)と呼ぶ。また、利用者が結託者であるか否かに関わらず、 r が $r \equiv u \bmod p_i$ を満足する場合、剰余 r は u に起因する可能性がある(possibly arise from)と呼ぶ。

【0117】(定義5) m 個の素数に対応する剰余の組(m -tuple of residues)の中の任意の k 個の剰余に対して中国剰余定理を適用したとき、これら m 個の剰余の組がすべて同一の利用者IDを与える場合、このような剰余の組を一貫している(consistent)と呼ぶことにする。

【0118】さらに、このような一貫している剰余の組の全ての剰余が、求められた結託者の利用者IDに起因している場合、この剰余の組は真に一貫している(truly consistent)と呼び、そうでない場合、この剰余の組は偽って一貫している(falsely consistent)と呼ぶことに

27

する。このような偽って一貫している組の簡単な例を以下に挙げる。

(検出アルゴリズム2)

(1) 検出された符号 $x \in \{0, 1\}^L$ を入力する。ここで、 $L = (p_{ave} - 1) k' t$ とする。

(2) x を k' 個の制限 $x \mid c_i, i = 1, \dots, k'$ 個に分解する。

(3) $i = 1$ から k' まで以下を実行する：

(3-1) 検出アルゴリズム1を $x \mid c_i$ に適用する。

(4) 全ての剰余の m 組に対して以下を実行する： * 10

$$\left[1 - \left\{ 1 - \left(1 - \frac{1}{p} \right)^k \right\} \right]^{k \cdot Ck + z \cdot 2^{k+z}} > 1 - \frac{\varepsilon}{2} \quad (4)$$

【0121】このとき、符号サイズは、 $L = (p_{ave} - 1) k' t$ で与えられる。

【0122】(補題1) 符号 $\Gamma(p_1, \dots, p_{k'}; n, t)$ の k' 個の剰余対の中には、少なくとも $2k' / c$ 個の剰余を起因させている結託者が少なくとも1人存在する。

(補題1の証明) 符号 $\Gamma(p_1, \dots, p_{k'}; n, t)$ の k' 個の剰余対に含まれる剰余は $2k'$ 個ある。平均すると、結託者1人あたり $2k' / c$ 個の剰余を起因させていることになる。従って、少なくとも1人の結託者は、 $2k' / c$ 個以上の剰余を起因させている。

【0123】(補題1の一般化) 補題1は、各成分符号から検出できる整数要素(剰余)の個数 q を $q = 2$ とした場合の例であるが、これを q を用いて一般化すると、次の通りとなる。

【0124】(一般化した補題1の証明) 符号 $\Gamma(p_1, \dots, p_{k'}; n, t)$ の k' 個の剰余 q 対(対ではないが、ここでは便宜上、そう呼ぶことにする)に含まれる剰余は、 qk' 個ある。平均すると結託者1人あたり、 qk' / c 個の剰余を起因させていることになる。従って、少なくとも1人の結託者は、 qk' / c 個以上の剰余を起因させている。

【0125】ここで、結託者ID(結託者の利用者ID)の再構成と検定には、 $(k+z)$ 個の剰余が必要なので、一般化した補題1の結果より、 $qk' / c \geq k+z$ が成立する必要がある。左辺の因子 q/c を右辺に移すと、条件式 $k' \geq c(k+z)/q$ を得る。実際には、 k' は整数であるので、 $k' \geq \lceil c(k+z)/q \rceil$ である。

【0126】(補題2) $t \geq \log_2(2k' / \varepsilon)$ とする。*

$$\Pr[x] = \begin{cases} \left(1 - \frac{x}{p}\right)^c - \left(1 - \frac{x+1}{p}\right)^c & \text{for } x \neq p-1 \\ \left(\frac{1}{p}\right)^c & \text{for } x = p-1 \end{cases} \quad (5)$$

【0131】(補題4) 以下の条件が成り立つとき、偽に一貫している剰余の $(k+z)$ 組が存在する確率は次式

* (4-1) もし、剰余の m 組が一貫しているならば、以下を実行する：

(4-2) その解を結託者として出力し中止する。

(5) 結託者が検出されなかったと出力する。

【0119】(定理2) $t \geq \log_2(4k' / \varepsilon)$ とする。

以下の方程式が成立するとき、符号 $\Gamma(p_1, \dots, p_{k'}; n, t)$ は ε 誤りを持った c -secure 符号である。

【0120】

【数11】

※符号 $\Gamma(p_1, \dots, p_{k'}; n, t)$ に対して先の検出アルゴリズム1を適用するとき、 k' 個の剰余対の検出誤り率(k' 個の剰余対の中に、どの結託者にも起因しない剰余が含まれてしまう確率)は、 ε 以下である。

【0127】(補題2の証明) ある構成要素 $\Gamma_0(p_i, t)$ に対して検出アルゴリズム1を適用するときは、定理1より $t \geq \log_2(2k' / \varepsilon)$ ならば、剰余対の検出誤り率は ε / k' 以下である。全部で k' 個の構成要素が存在するので、全ての剰余対に対する検出誤り率は ε 以下である。

(補題3) ある一貫した剰余の m 組が存在しており、これに別の因数 p に対する剰余対からの剰余を加えて剰余の $(m+1)$ 組を構成するとき、この $(m+1)$ 組の剰余が偽に一貫している確率は、 $1 - (1 - 1/p)^c$ 以下である。

【0128】(補題3の証明) 各剰余対は、全ての結託者の利用者IDに対する q を法とする剰余のうちの最大値と最小値により構成されている。利用者は自分の利用者IDを知らないの、結託が行われたとき、ある利用者IDが結託者のものである確率は、利用者IDによらず一様であると考えられる。従って、ある結託者の剰余がある値をとる確率は、等しく $1/p$ である。

【0129】 c 人の結託者の剰余が全て一様に分布するとき、最大の剰余がある値 $c \in \mathbb{Z}/p\mathbb{Z}$ をとる確率 $\Pr[x]$ は、以下のように与えられる。なお、 $\mathbb{Z}/p\mathbb{Z}$ は0以上、 p 未満の整数の集合である。

【0130】

【数12】

に示すように ε 以下である。

【0132】

【数13】

$$\left[1 - \left\{ 1 - \left(1 - \frac{1}{p} \right)^c \right\}^z \right]^{c(k+z)/2 \cdot Ck + z \cdot 2^{k+z}} \geq 1 - \varepsilon \quad (6)$$

【0133】(補題4の証明) k' 個の剰余対から剰余の $(k+z)$ 組を選択する組合せは、 $k' \cdot C_{k+z} \times 2^{k+z}$ 通りある。補題14から、剰余の $(k+z)$ 組が偽に一貫している確率は、 $(1 - (1 - 1/p)^c)^z$ である。従って、全ての組合せにおいて、少なくとも1個の偽に一貫 *

*している剰余の $(k+z)$ 組が現れる確率は、次のような上限が与えられる。

【0134】

【数14】

$$P_F \leq \left[1 - \left\{ 1 - \left(1 - \frac{1}{p} \right)^c \right\}^z \right]^{1/2 Ck + z \cdot 2^{k+z}} \quad (7)$$

【0135】補題1の条件式が成立するとき、確率 P_F は ε 以下である。

【0136】(定理2の証明) 潔白な利用者を誤って結託者であると検出する原因は、剰余対の検出誤りと、偽に一貫している剰余の組の選択の二つがある。それぞれの確率を $\varepsilon/2$ 以下とするならば、検出誤り率は ε 以下となる。補題2と補題4より、上の上限の式を得る。偽*

※に一貫している剰余の組を排除する確率を最小の因数で下限を抑える代わりに、小さい方から z 個の因数を用いて下限を抑えることで、式(4)に代えて次式(8)に示すような符号サイズのより小さな上限を得ることができる。

【0137】

【数15】

$$\left[1 - \prod_{i=1}^z \left\{ 1 - \left(1 - \frac{1}{p_i} \right)^c \right\} \right]^{c(k+z)/2 \cdot Ck + z \cdot 2^{k+z}} \geq 1 - \frac{\varepsilon}{2} \quad (8)$$

【0138】ここで、 p_1, \dots, p_z は $p_1, \dots, p_{k'}$ の中から選んだ z 個(ただし、 $p_1 < p_2 < \dots < p_z$ とする)であり、最も小さいものから順に選んだ z 個であってもよいし、 $k+z$ 番目から小さい順に最も大きい $k+z$ 番目まで選んだ z 個であってもよいし、あるいは最も小さいものから $k+z$ 番目に小さいものまでの中から選んだ z 個であってもよい。また、 $p_i (i=1, 2, \dots, k')$ は c 個の利用者IDに対して剰余計算部で計算される各剰余(整数要素)のとりうる値であり、本実施形態では前述の法記憶部21-1, 21-2, \dots , 21- k' で用意されている k' 個の素数である。

【0139】式(8)の意味について説明する。まず、式(8)の左辺は、検出が正しく結託者IDを特定する確率の下限を与えている。つまり、左辺の大括弧の肩に乗っている「べき」は、 k' 個の剰余対から $(k+z)$ 個の剰余を選択してくる場合の例である。その個々の選択に対して、結託者IDが正しいか否かの判定を正しく行う確率の加減が右辺全体の意味するところである。

【0140】ここで、式(8)左辺の大括弧の中身について詳しく説明する。上記の各選択では、結託者IDが正しいか否かを余分に z 個の剰余によって検定している。大括弧の中の Π による積の部分は、 z 個の検定すべて

が、誤った結託者IDを正しいとしてしまう確率の上限を与えている。なぜなら、各検定が誤った結託者IDを正しいと判定してしまう確率の下限は、(補題3)において、与えている確率 $1 - (1 - 1/p)^c$ において、各成分符号から検出できる整数要素(剰余)の個数 p をその剰余に対応する因数で置き換えたものによって与えられる。

【0141】検定に用いられる剰余に対応する z 個の因数は、最も小さな因数からなる組み合わせが p_1, p_2, \dots, p_z の場合であって、この組み合わせが、誤った検定を行う確率の下限を最大にする組み合わせである。よって、 Π による積部分が z 個の検定すべてが、誤った結託者IDを正しいとしてしまう確率の上限を与えていることになる。よって、式(8)は左辺であるところの正しい結託者IDを検出する確率の下限が右辺であるところの $1 - \varepsilon/2$ 以上であるための条件式を意味していることになる。このように本実施形態によると、前述した一般化した補題1によって与えられる条件式 $k' \geq (k+z)/q$ を満たすように、より好ましくは式(8)を満足するように成分符号の数 k' を規定することによって、結託攻撃への耐性を有し、かつ3人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づ

31

いて十分かつ適切な埋め込み符号を生成し、かつその埋め込み符号を正しく復号することができる。

【0142】次に、本実施形態における結託者を特定するアルゴリズムについて図9に示すフローチャートを用いて説明する。結託者ID計算部46は、成分符号復号部42-1、42-2、…、42-k'が出力したk'個の剰余対を入力する(ステップS1)。剰余対は、まず剰余選択部51に入力される。剰余選択部51は、各剰余対から一方の剰余を選択し、k個の剰余の組(R₁, R₂, …, R_k)を生成する(ステップS2)。

【0143】生成されたk'個の剰余の組は、一貫性検査部52に入力される。一貫性検査部52は、入力されたk'個の剰余の組から相異なるk個の剰余(S₁, S₂, …, S_k)を選択し(ステップS3)、中国剰余定理部53に渡す。

【0144】中国剰余定理部53は、中国剰余定理に従い結託者ID_uを計算する(ステップS4)。この中国剰余定理の計算は、図10のフローチャートに示す処理の流れに従って行われる。計算された結託者ID_uは、一貫性検査部52へ返される。

【0145】一貫性検査部52では、残りの(k' - k)個の剰余のうちの所定個数(z)の剰余との間に、 $R_i = u \bmod p_i$ (i = i₁, i₂, …, i_z)の関係が成立する場合があるか否かを判定する(ステップS5)。この関係が成立する場合、一貫性検査部52はuを結託者IDとして出力する(ステップS6)。この関係が成立しない場合には、この関係が成立するまで、ステップS3で入力されたk'個の剰余の組から新たな相異なるk個の剰余(S₁, S₂, …, S_k)を選択して中国剰余定理部53に渡す処理を行う。

【0146】ステップS7でk個の剰余(S₁, S₂, …, S_k)が最後の候補と判定されると、一貫性検査部52は剰余選択部51に対して新たなk'個の剰余の組を要求し(ステップS8)、ステップS5で $R_i = u \bmod p_i$ (i₁, i₂, …, i_z)の関係が成立するまでステップS3, S4, S7の処理を繰り返す。もし、ステップS7で新たなk個の剰余(S₁, S₂, …, S_k)の候補が存在しない場合には、結託者IDの特定に失敗したとする(ステップS9)。

【0147】最後に、図11に示すフローチャートを用いて本実施形態における埋め込み符号検出部14の処理の流れについて説明する。検出対象コンテンツ(例えば埋め込み済みコンテンツ)が入力され(ステップS11)、この検出対象コンテンツから埋め込み符号が抽出されると(ステップS12)、符号分割部41及び部分復号部42-1、42-2、…、42-k'を介して得られた成分符号に基づいて、結託判定部44-1、44-2、…、44-k'により結託の有無が判定される(ステップS13)。

【0148】ここで、結託判定部44-1、44-2、

32

…、44-k'のいずれでも結託が無いと判定されると、利用者ID計算部43により利用者IDが計算され(ステップS14)、この利用者IDが出力される(ステップS15)。

【0149】一方、ステップS13で結託判定部44-1、44-2、…、44-k'の少なくとも一つで結託があると判定されると、結託判定部45を介して結託存在信号が出力され(ステップS16)、かつ結託者ID計算部46で結託者IDが計算され(ステップS17)、この結託者IDが出力される(ステップS18)。

【0150】この場合、ステップS13での結託の有無の判定と、ステップS14での利用者IDの計算については、処理が簡単であり、高速に行うことができる。これに対して、ステップS17での結託者IDの計算には時間がかかるが、結託の有無の判定を先に行い、結託があったと判断された場合にのみ結託者IDの計算を行うことにより、無駄な計算を省略できる。

【0151】また、本発明の電子透かし検出装置を利用者機器に適用する場合には、結託の有無のみを判定し、その結果によって利用を中断させるなどの利用制御を行えばよいので、結託者の計算(特定)まで行う必要は必ずしもない。

【0152】このように本実施形態によると、埋め込むべき符号サイズを抑えつつ、利用者総数や結託者数が大きい場合についても、結託攻撃に対するロバスト性を持つことができる。

【0153】(第2の実施形態)図12は、本発明の第2の実施形態における埋め込み符号生成部11の構成を示している。本実施形態の埋め込み符号生成部11では、図3に示した構成にコンテンツの利用者を特定する利用者特定情報に対して利用者IDを割り当てる利用者ID割り当て部26と、利用者IDと利用者ID割り当て部26により割り当てられた利用者IDとを対応付けて格納した利用者特定情報/利用者ID対応テーブル27が追加されている。

【0154】利用者ID割り当て部26では、入力された利用者特定情報に対して後述するように利用者IDの割り当てが行われ、この割り当てられた利用者IDが剰余計算部22-1~22-k'に入力される。また、利用者特定情報/利用者ID対応テーブル27は、図13に示されるように、利用者ID割り当て部26は利用者ID候補生成部261、利用者ID候補判定部262及び利用者ID決定部263から構成される。図14に示すフローチャートを用いて、図13の利用者ID割り当て部26の処理手順を説明する。

【0155】まず、利用者特定情報を入力する(ステップS21)。利用者特定情報は、個々の利用者に対応してユニークな識別情報であり、例えば利用者の氏名が用いられる。利用者特定情報に対応して、利用者ID候補生成部261において利用者ID候補を一つずつ生成す

33

る(ステップS22)。利用者ID候補としては、まだ割り当てられていない(使用されていない)IDが用いられる。

【0156】次に、各利用者ID候補について弱IDか否かの判定を利用者ID候補判定部262において順次行う(ステップS23)。弱IDとは、複数の利用者ID候補のうちで結託者IDでない、つまり無実(結託者でない)の利用者の利用者IDであるにも関わらず、結託者IDとして誤検出される可能性のより高い利用者IDであり、誤検出に弱いIDという意味から、このように呼ぶものとする。このステップS23の判定の結果、利用者ID候補が弱IDである場合は、ステップS22に戻って次の利用者ID候補を生成し、再びステップS23の判定を行う。

【0157】ステップS23の判定の結果、利用者ID候補が弱IDでなければ、つまり結託者IDとして誤検*

$$\Pr[x;p,c] = \begin{cases} \left(1 - \frac{x}{p}\right)^c - \left(1 - \frac{x+1}{p}\right)^c & \text{for } x = p-1 \\ \left(\frac{1}{p}\right)^c & \text{for } x = p-1 \end{cases} \quad (9)$$

を定義する。次に、

※ ※ 【数17】

$$Q[x;p,c] = \Pr[x;p,c] + \Pr[p-1-x;p,c] \quad (10)$$

を定義する。ある利用者ID(uとする)が結託者IDとして誤検出される確率を概ね表す量として、次の評価値EEFを計算する。

★ 【0159】

【数18】

$$EEF = 1 - \prod_{\substack{j(1), j(2), \dots, j(k+1) \in \{1, 2, \dots, k\} \\ j(1) < j(2) < \dots < j(k+1)}} \left\{ 1 - \prod_{i=2}^{k+1} Q_{u_{p_i}; p_i, c} \right\} \quad (11)$$

【0160】ここで、 $u_p = u \bmod p$ とする。これ以外にも、ある利用者IDについて誤検出確率を近似する評価値が存在するならば、それを式(11)のEEFの代わりに用いることが可能である。例えば、次式(12)で表*

☆される評価値EEFを用いてもよい。

【0161】

【数19】

$$EEF = \sum_{i=0,1,\dots,k'} Q_{u_{p_i}; p_i, c} \quad (12)$$

【0162】次に、ステップS32で推定された誤検出確率(例えば、式(11)または(12)のEEF)が所定の閾値を超えたか否かを調べ(ステップS33)、閾値を超える場合は、利用者ID候補が弱IDであると判定し(ステップS34)、また誤検出確率が閾値以下の場合、利用者ID候補が非弱IDであると判定する(ステップS35)。

【0163】このようにして図12中に示した利用者ID割り当て部26では、入力された利用者特定情報に対して、複数の利用者ID候補の中から結託者IDとして誤検出されにくいID(非弱ID)が利用者IDとして割り当てられる。以後、こうして利用者ID割り当て部2

34

*出される可能性のより低い利用者ID(これを誤検出に弱くないIDという意味で、非弱IDという)であれば、利用者ID候補決定部263においてその利用者ID候補をステップS21で入力された利用者特定情報に割り当てる利用者IDに決定する(ステップS24)。

【0158】図15に示すフローチャートを用いて、利用者ID候補が弱IDか非弱IDかを判定するステップS23の判定処理の具体的な手順を説明する。まず、ステップS22で生成された利用者ID候補を一つずつシークエンシャルに入力し(ステップS31)、この利用者ID候補が結託者IDとして誤検出される確率(誤検出確率)を推定する(ステップS32)。この誤検出確率の推定は、例えば前述した p_i, k, k', c といったパラメータを用いて次のようにして行われる。まず、

【数16】

6で割り当てられた利用者IDに対して、第1の実施形態と同様に剰余計算部22-1~22-k'、成分符号生成部24-1~24-k'及び符号連接部25により順次処理が行われることによって、埋め込み符号が生成される。

【0164】言い換えれば、利用者ID割り当て部26においては、入力された利用者特定情報に対して、複数の利用者ID候補の中から結託者IDとして誤検出されやすい弱IDを利用者IDに割り当てないようにすることによって、誤検出の確率を小さくすることができる。仮に、弱IDが結託者IDとして検出されたとしても、それは結託者IDとして見なさないことにすればよい。

35

【0165】ところで、弱IDは埋め込み符号の符号長の決定に大きな影響を与える。電子透かし検出装置においてある利用者IDが検出されたとき、それがたとえ弱IDであったとしても誤検出確率をある許容される確率より小さくするためには、非常に多数の因数からなる因子基底(具体的には、法記憶部21-1, 21-2, ..., 21-k'に記憶される互いに素の関係にある整数、例えば相異なるk'個の素数 p_i ($i=1, 2, \dots, k'$))を用意する必要がある。しかし、弱IDを排除しない場合に、ある埋め込み符号がある誤検出確率を持つ*10

$$\begin{aligned} \text{detect}(u) = & \text{detect}(u) \wedge \text{weak}(u) \wedge \text{collude}(u) \\ & \vee \text{detect}(u) \wedge \text{weak}(u) \wedge \neg \text{collude}(u) \\ & \vee \text{detect}(u) \wedge \neg \text{weak}(u) \wedge \text{collude}(u) \\ & \vee \text{detect}(u) \wedge \neg \text{weak}(u) \wedge \neg \text{collude}(u) \end{aligned} \quad (13)$$

であるから、

※ ※ 【数21】

$$\begin{aligned} \text{Pr}[\text{detect}(u)] = & \text{Pr}[\text{detect}(u) \wedge \text{weak}(u) \wedge \text{collude}(u)] \\ & + \text{Pr}[\text{detect}(u) \wedge \text{weak}(u) \wedge \neg \text{collude}(u)] \\ & + \text{Pr}[\text{detect}(u) \wedge \neg \text{weak}(u) \wedge \text{collude}(u)] \\ & + \text{Pr}[\text{detect}(u) \wedge \neg \text{weak}(u) \wedge \neg \text{collude}(u)] \end{aligned}$$

(14)

となる。これらのうち誤検出率に寄与するのは、式(14)右辺の第2項と第4項である。符号長を短くするには、誤検出率を低下させることなく、より小さな個数(k')の因数によって結託者ID候補の検定を行うことができるような方法を採用すればよい。ここで、単純により小さな個数の因数によって結託者ID候補の検定を行う場合は、式(14)右辺の第4項の確率はさほど変化しないが、第2項の確率は大きく増加してしまい、誤検出確率が増加してしまう。

【0167】しかし、前述したように弱IDを予め利用者IDとして割り当てないように排除しておけば、式(14)右辺の第2項は誤検出確率には組み込まれない。後述する埋め込み符号検出部14において結託者ID候補の利用者IDリストを用意しておき、その利用者IDリストの中から同じIDを取り出していけば、やがて非弱IDが得られる確率が高いので、それを結託者IDと決定することにすれば、結果的に短い符号長の埋め込み符号を生成できることになる。

【0168】図16は、第2の実施形態における埋め込み符号検出部14の構成を示している。本実施形態では、第1の実施形態と同様に図6で説明した符号分割部41を経て成分符号復号部42-1, 42-2, ..., 42-k'で得られた利用者IDに対応するk'個の剰余対が結託者ID計算部47に入力される。

【0169】結託者ID計算部47で計算された結託者IDは、結託者特定情報生成部49に入力され、この結託者特定情報生成部48において図12で説明した利用者特定情報/利用者ID対応テーブル27を参照して結

36

*場合、弱IDを利用者IDから排除することによって、より少数の因子からなる因子基底を持つ埋め込み符号によって同等の誤検出確率を実現できる。

【0166】このことは、次のように説明できる。ある利用者IDをuとし、このuが検出されるという事象をdetect(u)、uが弱IDであるという事象をweak(u)、uが結託者IDであるという事象をcollude(u)と表すことにする。このとき、

【数20】

託者特定情報が生成される。結託者ID計算部47は、図6中に示した結託者ID計算部46と異なり、利用者IDを以下のようにして計算する。

【0170】図17に示されるように、結託者ID計算部47は結託者ID候補生成部471、結託者ID候補判定部472及び結託者ID決定部473から構成される。以下、図18に示すフローチャートを用いて、図17の結託者ID計算部47の処理手順を説明する。

【0171】まず、結託者ID候補生成部471の処理について説明する。成分符号復号部42-1, 42-2, ..., 42-k'で得られたk'個の剰余対を入力する(ステップS41)。次に、既に使用されている全ての利用者IDをj($j=0 \sim n-1$)として、まず、 $j=0$ に設定する(ステップS42)。次に、現在設定されているjが利用者IDの範囲を越えているか($j > n-1$)否か($j \leq n-1$)を判定する(ステップS43)。jが利用者IDの範囲を越えている場合には、結託者IDの計算を終了する。

【0172】一方、jが結託者IDの範囲を越えていない場合には、その利用者ID(j)について、図18のステップS41で入力されたk'個の全ての剰余対に対して、いずれかの剰余($r_i^{(+)}$ または $r_i^{(-)}$)に対する p_i を法とする合同式 $j \equiv r_i^{(\pm)} \pmod{p_i}$ を満足している場合の数xを計数する(ステップS44)。以下、この場合の数xを「合同式充足数」と呼ぶ。

【0173】次に、この合同式充足数(x)が所定の閾値y以上かどうかを調べる(ステップS45)。この閾値yの値は、検出誤りを小さくしたい場合には大きな値

37

を、検出誤りが大きくて良い場合には大きな値をそれぞれ設定することができる。以下で説明するような、結託者ID候補に対して弱IDか否かによる判定を行う場合には、 y として $k+z$ よりも小さな値に設定した場合でも、検出誤りを ε 以下とできることがある。しかし、そのような判定を行わない場合には、 y は $k+z$ 以上の値に設定しないと、検出誤りを ε 以下にできない。

【0174】合同式充足数 x がこの閾値 y 以上の場合には、 j は結託者ID候補であると決定する(ステップS46)。一方、 x が閾値 y より小さい場合には、後述するステップS49に進む。こうして生成された結託者ID候補が、結託者ID候補生成部471より出力される。

【0175】次に、結託者ID候補判定部472の処理について説明する。結託者ID候補生成部471が生成した結託者ID候補は、弱IDであって、本当の結託者IDではない恐れがある。そこで、結託者ID候補判定部472は、こうして生成された結託者ID候補 j が弱IDであるか否かを判定する(ステップS47)。弱IDとは、前述したように結託者IDでないにもかかわらず、結託者IDとして誤検出される可能性のより高い利用者IDである。一方、結託者IDとして誤検出される可能性のより低い利用者IDを非弱IDと呼ぶ。

【0176】最後に、結託者ID決定部473の処理について説明する。結託者ID候補判定部472におけるステップS47の判定の結果、結託者ID候補が弱IDでなければ、つまり、結託者IDとして誤検出される可能性のより低い利用者IDであれば、結託者ID決定部473によって、その結託者ID候補を結託者IDに決定する(ステップS48)。一方、ステップS47の判定の結果、結託者ID候補が弱IDである場合には、ステップS49に進む。

【0177】以上は、 j の一つの値に対して行われる処理である。ステップS49では、次の j について同様の処理を行うため、 j を1だけ増加させる。その後、ステップS43に戻り、同様の処理を繰り返す。従って、図19の結託者ID候補生成処理は、すべての利用者IDに対して行われ、 $x \geq y$ となる j が全て結託者ID候補として求められる。

【0178】次に、図19に示すフローチャートを用いて、上記のようにして生成された結託者ID候補について弱IDか非弱IDかを判定する図18のステップS47の判定処理の具体的な手順について説明する。この判定処理は、基本的に図12に示した埋め込み符号生成部11において利用者ID割り当て部26における図13の利用者ID候補判定部262の図15で示した判定処理と同様であり、判定の対象が利用者ID候補から結託者ID候補に置き換わっただけである。

【0179】すなわち、まず図18のステップS46で決定された結託者ID候補を一つずつシーケンシャルに

38

入力し(ステップS61)、これらの結託者ID候補が結託者IDとして誤検出される確率(誤検出確率)を推定する(ステップS62)。この誤検出確率の推定は、例えば先の式(9)(10)を定義し、ある利用者ID(u)が結託者IDとして誤検出される確率を概ね表す量として、式(11)または式(12)の評価値EEFを計算することによって行う。次に、ステップS62で推定された誤検出確率(例えば、式(11)または(12)のEEF)が所定の閾値を超えたか否かを調べ(ステップS63)、閾値を超える場合は、結託者ID候補が弱IDであると判定し(ステップS64)、また誤検出確率が閾値以下の場合は、結託者ID候補が非弱IDであると判定する(ステップS65)。

【0180】図20は、本実施形態において各パラメータが $L=7.34 \times 10^6$ 、 $c=32$ 、 $EEF=0.000001$ 、 $k=2$ 、 $p_0=512$ 、 $z=11$ 、 $k'=208$ 、 $n=2.63 \times 10^5$ の場合に、実際の結託者IDに対して検出される結託者IDと、先の合同式充足数(x)と、検出結果の正誤(1が正検出、0が誤検出)を示している。

【0181】この例では、 $k+z=13$ であるので、第1の実施形態では実際の結託者IDのうちID=47824だけが結託者IDとして検出される。これに対し、本実施形態では実際の結託者IDのうち、それが非弱IDであって、かつ充足式数 x が比較的多いIDは正しく結託者IDとして検出される。図20の例では、結託者IDのうち例えば3桁を超えるIDを非弱IDとすれば、これらの非弱IDのうち充足式数 x が10以上のものは、全て結託者IDとして検出される。

【0182】図21は、本実施形態においてパラメータ L 、 c 、 EEF 、 k 、 p_0 、 z 、 k' 及び n のうち結託者数 c 以外は図20と同じにし、 $c=64$ とした場合に、実際の結託者IDに対して検出される結託者IDと、先の合同式充足数(x)と、検出結果の正誤(1が正検出、0が誤検出)を示している。結託者数 c が図20の場合の2倍となっているので、第1の実施形態では結託者IDを検出することはできない。これに対し、図21の例では、結託者IDのうち例えば5桁以上のIDを非弱IDとすれば、これらの非弱IDのうち充足式数 x が6以上のものは、全て結託者IDとして検出される。

【0183】このように本実施形態によると、以下の効果を得ることができる。

(1)より大きな結託者数 c に対しても、結託者数を特定できる。言い換えれば、想定する最大の結託者数が同じならば、第1の実施形態に比較してより短い符号長の埋め込み符号を実現することができる。

(2)複数の結託者IDを特定できる。

(3)埋め込み符号に結託攻撃以外のノイズ(例えば、ランダムノイズ)が加わっても、結託者を特定できる。

【0184】ここで、(1)(2)は前述した通りである

が、(3)の効果について補足すると次の通りである。埋め込み符号(透かし情報)に例えばコンテンツ全体にわたってランダムなノイズが加わると、成分符号の復号時に誤った剰余を出力する符号が生じることがある。このようなランダムノイズによる誤り率がある程度までならば、正しい剰余対の数の方が圧倒的に多い。従って、上述した合同式充足数は、誤った結託者ID候補よりも正しい結託者ID候補の方が大きいため、結託者IDの誤検出率は小さいことになる。

【0185】(第3の実施形態)図22に、本発明の第3の実施形態における埋め込み符号生成部11の構成を示す。本実施形態の埋め込み符号生成部11では、図3に示した構成にデータベース参照部28及び非弱IDデータベース29が追加されている。

【0186】非弱IDデータベース29は、全ての利用者ID候補のうち非弱IDを格納している。この非弱データベース29に格納される非弱IDは、第2の実施形態の利用者ID候補判定部262における判定方法と同様の方法、例えば図15で説明したアルゴリズムによって全ての利用者ID候補について弱IDか非弱IDかの判定を行うことによって得られる。

【0187】データベース参照部28は、利用者特定情報が入力されると、この利用者特定情報に対応して非弱IDデータベース29内の一つの非弱IDを利用者IDとして割り当て、その非弱ID(利用者ID)を出力する。この利用者IDに対して、第1及び第2の実施形態と同様に剰余計算部22-1~22-k'、成分符号生成部24-1~24-k'及び符号接続部25により順次処理が行われることによって、埋め込み符号が生成される。

【0188】非弱IDデータベース29には、データベース参照部28で利用者特定情報にどの非弱IDを割り当てたかを示す情報が併せて格納される。すなわち、非弱IDデータベース29に格納される非弱IDのうち、既に利用者特定情報に対して利用者IDとして割り当てられた非弱IDには、対応する利用者特定情報が対応付けて格納される。これにより以後に入力される利用者特定情報には、既に他の利用者特定情報に対して割り当てが行われた非弱IDは割り当てられない。

【0189】このように本実施形態の埋め込み符号生成部11によると、非弱ID、すなわち全ての利用者IDのうちで結託者IDとして誤検出される可能性の低い利用者IDを予め求めて、これらを非弱IDデータベース29に格納しておき、この非弱IDデータベース29を参照して利用者特定情報に対する利用者IDの割り当てを行うため、第2の実施形態と同様の利用者ID割り当て処理を少ない処理量で、短時間を実現することができる。

【0190】図23は、本実施形態における埋め込み符号検出部14の構成を示している。本実施形態の埋め込

み符号検出部14は、図16に示した利用者特定情報/利用者ID対応テーブル27と結託者特定情報生成部48に代えて、非弱IDデータベース29とデータベース参照部49が追加されている。

【0191】非弱IDデータベース29は、図22で説明した通りであり、非弱IDと利用者特定情報を対応付けて格納している。データベース参照部49は、結託者ID候補生成部47から結託者ID候補が入力されると、非弱IDデータベース29に格納されている非弱IDのうち、結託者ID候補のいずれかに合致する非弱IDを結託者IDと決定し、その非弱IDに対応する利用者特定情報を非弱IDデータベース29から読み出して、これを結託者特定情報として出力する。

【0192】本実施形態の埋め込み符号検出部14によると、非弱ID、すなわち全ての利用者IDのうちで結託者IDとして誤検出される可能性の低い利用者IDを予め求めて、これらを非弱IDデータベース29に格納しておき、この非弱IDデータベース29を参照して結託者IDの計算と結託者IDに対応する利用者特定情報の算出を行うため、第2の実施形態と同様の結託者ID計算の処理を少ない処理量で、短時間を実現することができる。

【0193】ここでは、非弱IDを弱IDと判別するために非弱IDデータベース29を用いたが、回路やプログラムとして弱IDと非弱IDとの判別を行うようにしてもよい。特に、結託者IDが分かればそれから結託者を特定することが本発明以外の手段により可能である場合には、単に弱IDの排除のみを行えばよい。

【0194】(第4の実施形態)次に、本発明の第4の実施形態として、ある条件の下で実現できる、第2の実施形態よりも短い符号サイズのc-secure符号による電子透かし埋め込み装置及び検出装置について説明する。

【0195】図24は、本実施形態に係る電子透かし埋め込み装置における埋め込み符号生成部の構成を示すブロック図である。この埋め込み符号生成部は、利用者IDを入力して同値類に基づく成分符号を生成する成分符号生成部61-1, 61-2, ..., 61-k'と、これらの各成分符号を一つの符号に接続することによって、透かし情報である埋め込み符号を生成する符号接続部62からなる。

【0196】図25に、図24に示した同値類に基づく成分符号生成部61-1, 61-2, ..., 61-k'の一つ(61-i)の構成を示す。以下、 $Z/pZ = \{0, 1, 2, \dots, p-1\}$ とする。成分符号生成部61-iは、 $(Z/pZ)^k$ 内対応点計算部611と同値類要素番号計算部612及び成分符号生成部613によって構成される。

【0197】 Z/pZ 内対応点計算部611は、利用者IDを入力して、対応する Z/pZ 内の点を出力する。利用者ID u と $(Z/pZ)^k$ 内の点 $(u_0, u_1, u_2,$

41

..., u_{p-1})との対応付けは、例えば、 $u = u_0 + u_1 p + \dots + u_{k-1} p^{k-1}$ によって行う。ある集合Uの要素に間に同値関係Rがあるとき、その同値関係Rによってある要素uと同値なものの全体の集合をその要素uの同値類と呼ぶ。Uの同値関係Rに関する同値類全体からなる集合を U/R で表し、UのRに関する同値類という。 $(Z/pZ)^k$ の要素の間にある平行移動Tによって、同値関係 R_T が定義できる。そして、この同値関係 R_T に関する同値類が定義できる。

【0198】一つの同値類に属する要素に対して、0から $p^{k-1}-1$ まで番号(これを同値類要素番号と呼ぶことにする)を割り振ることができる。同値類要素番号計算部612は、この同値類番号を計算して部分IDとして出力する。すなわち、本実施形態では入力された利用者IDに対する整数要素の組として、同値類要素番号計算部612により同値類要素番号が計算される。成分符号生成部613は、同値類要素番号計算部612で計算された部分IDから成分符号を生成する。

【0199】図26は、平行移動による同値類の例を示す図である。これは $p=7$ 、 $k=2$ の例である。平行移動(1, 6)と平行移動(3, 4)は、斜線部で示される格子によって構成されている同じ同値類を定義していることが分かる。

【0200】図27は、図26の $p \times p$ の格子を周期的に繰り返したとき、同値類がどのように表されるかを示す図である。平行移動による同値関係によって定義される同値類であって、(0, 0)の格子を含む同値類は、ある傾きを持った直線上に乗っていることが分かる。図28は、図26を $k=3$ に拡張した場合の例を示す図であ*

$$\sum_{j=0}^{k-1} u_j a_{i,j} \bmod p$$

【0207】図29に、本実施形態に係る電子透かし検出装置における埋め込み符号検出部の構成を示す。この埋め込み符号検出部は、符号分割部71、同値類に基づく成分符号復号部72-1、72-2、..., 72-k'及び結託者ID計算部73から構成されている。

【0208】図示しない埋め込み符号抽出部により、入力された検出対象コンテンツ(埋め込み済みコンテンツ)から透かし情報(埋め込み符号)が抽出され、この抽出された透かし情報である埋め込み符号が符号分割部71により各成分符号に分割された後、同値類に基づく成分符号復号部72-1、72-2、..., 72-k'により復号されることにより、利用者IDに対応する同値類要素番号の対が生成される。こうして生成された各同値類要素番号の対から、結託者ID計算部73で結託者IDが計算され、結託者が特定される。

【0209】なお、第1、第2の実施形態と同様に、同値類要素番号の対の一方から利用者ID計算部により利用者IDを求め、また各同値類要素番号の対から結託判

42

*る。同様にして、任意の正整数kに対して平行移動による同値関係によって同値類を定義することができる。

【0201】一つの同値類に含まれる元の個数は、p個である。順序番号(同値類内要素番号)は、このp個の元に対して与えられる。一方、商集合の要素の個数(=同値類の個数)は $p^k/p = p^{k-1}$ である。従って、順序番号を指定すると、 p^{k-1} 個の元が指定されることになる。この順序番号が部分IDとして成分符号によって符号化されることになる。

【0202】ここで、同値類要素番号計算部612での同値類要素番号(部分ID)の割当て方法について述べる。この割当て方法として、次の2通りが考えられる。

【0203】(割当て方法1) 同値関係 R_A に関する同値類に対して割り当てた番号である同値類番号を用いる方法であり、0から $p^{k-1}-1$ までの番号が割り当てられる。

【0204】(割当て方法2) 同値類の要素に対して割り当てた番号を用いる方法であり、0から $p-1$ までの番号が割り当てられる。

【0205】これらのうち割当て方法2がより好ましい。この割当て方法1を採用した場合には、第2の実施形態と同様の議論が展開できるため、先の式(6)が成立する。つまり、式(6)と後述する式(22)の両者を満足するような符号を採用すれば良い。この割当て方法2の例を挙げる。平行移動 $A_i = (a_{i,0}, a_{i,1}, \dots, a_{i,k-1})$ による同値類の場合、 $u = (u_0, \dots, u_{k-1})$ は、同値類要素番号(部分ID)として次式が割り当てられる。

【0206】

【数22】

(15)

定部により結託の有無を判定し、その結託判定部判定結果について、結託判定OR部で論理和をとることにより、結託が存在したか否かを最終的に判定して、結託が存在すると判定されたときに結託者ID計算部73で結託者IDを計算する構成としてもよい。

【0210】図30は、同値類に基づく成分符号復号部72-1、72-2、..., 72-k'の一つ(72-i)の構成を示している。同値類に基づく部分復号部72-iは、後述するランダム誤りを許容する検出アルゴリズム3に基づくものであり、ブロック分割部720、“1”ビット計数部721、“ $> t_0$ ”判定部722、“ $< d - t_0$ ”判定部723、最小位置決定部724及び最大位置決定部725から構成される。

【0211】ブロック分割部720は、入力された成分符号を各ブロックへ制限したものに分割して分割結果をそれぞれ“1”ビット計数部721へ出力する。“1”ビット計数部721は、“1”が立っているビットの数を計数して、その計数値を“ $> t_0$ ”判定部722及び

43

“ $< d - t_0$ ”判定部 723へそれぞれ出力する。

【0212】“ $> t_0$ ”判定部 722は、入力第1の閾値 t_0 より大きいかなかを判定し、真ならば1、偽ならば0をそれぞれ出力する。“ $< d - t_0$ ”判定部 723は、入力第2の閾値 $d - t_0$ より小さいかなかを判定し、真ならば1、偽ならば0をそれぞれ出力する。

【0213】最小位置決定部 724は、“ $> t_0$ ”判定部 722からの入力ビットの組のうち1が立っている最小のビット番号を出力する。最大位置決定部 725は、“ $< d - t_0$ ”判定部 723からの入力ビットの組のうち1が立っている最大のビット番号を出力する。

【0214】ここで、図29の電子透かし検出装置において埋め込み符号である透かし情報の復号時に誤りが生ずる可能性がある場合について説明する。埋め込み符号の復号時に誤りがある場合には、誤った利用者を結託者と特定するおそれがある。この誤りを防ぐには2通りの方法がある。

【0215】(方法1) 電子透かし埋め込み装置において、埋め込み符号に対して誤り訂正符号化を行ってから埋め込みを行い、電子透かし検出装置において検出された符号に対して誤り訂正復号を行う。

(方法2) 図29の成分符号復号部 72-1, 72-2, ..., 72-k' に誤りを許容する性質を持たせる。

【0216】本実施形態では、(方法2)を採用する。抽*

$$\varepsilon_1 = \sum_{i=t_0+1}^d {}_d C_i (1-\varepsilon_0)^{d-i} \varepsilon_0^i < e^{-\frac{(t_0-d\varepsilon_0)^2}{d}} \quad (16)$$

【0220】一方、結託によって改竄が行われたブロックに対して、結託以外の原因でランダムな誤りが加法的に加わった場合、 t_0 ビット以下の反転が生ずる確率

$$\varepsilon_2 = \sum_{i=0}^{t_0} {}_d C_i (1/2)^d < e^{-\frac{(\frac{d}{2}-t_0)^2}{d}} \quad (17)$$

【0222】ランダム誤りのために埋め込み符号を誤って検出をしてしまう確率は、少なくとも一つのブロックにおいて誤った検出をする確率以下であり、この確率は、

$$\varepsilon_3 = 1 - (1 - \varepsilon_1)^{n-1} (1 - \varepsilon_2)^2 < (n-1) \varepsilon_1 + 2 \varepsilon_2 \quad (18)$$

で表される。図31に示すように t_0 を適当に選択することで、加法的にランダムな誤りが加わった場合にも、検出誤りを小さく設定できる。図30に示した成分符号復号部 72-iは、上述したようなランダム誤りを許容する先の検出アルゴリズム3に基づく処理を行う。

【0223】図32に、結託者ID計算部74の構成を示す。結託者ID計算部74は、同値類選択部81、一貫性検査部82及び候補ID計算部83から構成される。

44

*出された埋め込み符号には誤り確率のランダムな誤りが加わっていると仮定する。第2の実施形態で述べた検出アルゴリズム1に改良を加えた以下のような検出アルゴリズム3を用いることで、誤りを許容する。

【0217】(検出アルゴリズム3)

(1) 検出された符号 $x \in \{0, 1\}^l$ を入力する。ここで、 $z = (n-1)d$ とする。

(2) $s = 0$ から $n-2$ まで、以下を実行する：

(2-1) もし、 $\text{weight}(x|_{B_s}) > 0$ ならば、中断する。

(3) $t = n-2$ から s まで、以下を実行する：

(3-1) もし、 $\text{weight}(x|_{B_t}) < d - t_0$ ならば、中断する。

(4) s と t を出力する。

ここで t_0 は、この検出アルゴリズム3の誤りに対する許容性を表すパラメータである。

【0218】次に、結託による埋め込み符号の改竄があったことを判定する閾値として、新たなパラメータを加える意味について説明する。埋め込み符号のうち、結託によっては改竄が行われなかったブロックに対して、結託以外の原因でランダムな誤りが発生した場合、 $t_0 + 1$ ビット以上の反転が生ずる確率は、次式で与えられる。

【0219】

【数23】

※は、次式より小さい。

【0221】

【数24】

【0224】同値類要素選択部81は、 k' 個の同値類要素番号の対の各々から一方の同値類番号を選択して一貫性検査部82へ出力し、一貫性検査部82から次候補の要求を受けると、同値類要素番号の新たな組を選択する。

【0225】一貫性検査部82は、 k' 個の組から $(k+1)$ 個の組を選択し、その同値類要素番号の組が真に一貫しているかなを検査する。この検査は、 $(k+1)$ 個のうち k 個の同値類要素番号を候補ID計算部83に渡し、返された候補IDが残りの同値類要素番号の示す同値類番号と矛盾していないかなかを判定することにより行われる。残りの個のすべての同値類番号に対して、この判定が矛盾していないという結果ならば、この候補IDを結託者IDとして出力し、そうでない場合には、次候補を一貫性検査部82に要求する。

45

【0226】ここで、図32中の候補ID計算部83においてk個の同値類要素番号から結託者IDを再構成する方法を示す。例えば、k個の平行移動 $A_{i(0)}, \dots, A_{i(k-1)}$ に対して、同値類要素番号が r_0, \dots, r_{k-1} で与

$$\sum_{j=0}^{k-1} u_j a_{i(v),j} = r_v \bmod p \quad (18)$$

【0228】k次正方行列 $(a_{i(v),j})$ が正則ならば、逆行列 $(a^{-1}_{j,i(v)})$ が存在する。この場合、次式によって利用者IDが得られる。

$$u_j = \sum_{v=0}^{k-1} a^{-1}_{j,i(v)} r_v \bmod p \quad (19)$$

【0230】一般には、正則性が満たされるとは限らない。正則性が満足されない場合には、利用者IDは一意に決まらず、結託者IDを含む利用者IDの集合が得られる。この集合は、pのべき乗の大きさを持つ。正則性を満たさない成分符号の組はあらかじめ分かっているの

※【0229】
【数26】

※10

★【0231】図32中の一貫性検査部82は、こうして得られた結託者IDの候補(を含む集合に対して)と、さらにz個の同値類要素番号 r_k, \dots, r_{k+z-1} との間の一貫性を検証する。それは、 $v=0, \dots, z-1$ に対して、次式が成立することを確認することで行われる。

【0232】
【数27】

★20

$$\sum_{j=0}^{k-1} u_j a_{i(k+v),j} = r_{k+v} \bmod p \quad (20)$$

【0233】本実施形態によると、第1、第2の実施形態と同様に結託攻撃への耐性を有し、かつ3人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成し、かつその埋め込み符号を正しく復号することが可能となる。以下、詳細に説明する。

【0234】まず、pを正整数とする。すなわち、本実施形態では第2の実施形態における $p_i (i=1, 2, \dots, k')$ (所定個数nの利用者IDに対して計算される剰余の値の個数)に相当する個数(所定個数nの利用者IDに対して計算される整数要素の値の個数)を同一の正整数pとしている。そして、利用者IDuを $u = u_0 + u_1 p + \dots + u_{k-1} p^{k-1}$ に従って、 $(u_0, u_1, \dots, u_{k-1}) \in (\mathbb{Z}/p\mathbb{Z})^k$ で表現する。また、 $k' = c(k+z)/2$ とし、 $p^k \geq n$ とする。

【0235】空間 \mathbb{Z}_p^k の平行移動 $A \equiv (a_0, a_1, \dots, a_{k-1})$ に関する同値関係 R_A を以下のように定義する。
 $R_A((u_0, u_1, \dots, u_{k-1}), ((u'_0, u'_1, \dots, u'_{k-1})))$
 $\longleftrightarrow u'_0 \equiv u_0 + a_0 \bmod p,$
 $u'_1 \equiv u_1 + a_1 \bmod p, \dots,$
 $u'_{k-1} \equiv u_{k-1} + a_{k-1} \bmod p$
 $jA = (ja_0 \bmod p, ja_1 \bmod p, \dots, ja_{k-1} \bmod p)$ とすると、jが $\gcd(j, p) = 1$ を満たすときには、 R_A と R_{jA} とは同じ同値関係を与える。

【0236】利用者全体の集合を $U = (\mathbb{Z}/p\mathbb{Z})^k$ の同値関係 R_A に関する商集合 U/R_A が定義できる。この商集合の個々の元は同値類と呼ばれ、同値関係 R_A によ

*えられた場合、次式の連立合同方程式が成り立つ。
【0227】
【数25】

46

て同一視された元の集合である。すべての同値類に対して、それに含まれる元に順序番号を与えることにより、ある番号を指定することで、各同値類から1個ずつ元を選択できる。

【0237】 $k' (k' \geq k)$ 個の平行移動 $A_0, \dots, A_{k'-1}$ を用意すると、それぞれに対して商集合 $Q_i = U/R_{A_i} (i=0, \dots, k'-1)$ が定義される。各商集合に対して、上に述べた順序番号を定義する。

【0238】次に、 k' 個の商集合中の任意のk個の商集合のそれぞれに対して、順序番号を指定することで、利用者を一意に特定できるような商集合の組を構成するために、以下のような条件を仮定する。

【0239】(条件1) 商集合の大きさを等しいとする。すべての $A_i = (a_{i,0}, \dots, a_{i,k-1}) (i=0, \dots, k'-1)$ において、すべての $a_{i,m} (m=0, \dots, k-1)$ に対して、 $\gcd(a_{i,m}, p) = 1$ または $a_{i,m} = 0$ であるとす

40

る。これにより、 $jA_i = (0 \bmod p, \dots, 0 \bmod p)$ を満たす最小の正整数jはpとなる。
 (条件2) 2つの平行移動 $A_i, A_{i'}$ に対して、 $jA_i = j'A_{i'}$ が成立する正整数 $j < p, j' < p$ が存在しない。pが素数の場合、このような条件を満たす平行移動の個数は、次のように数え上げることができる。まず、(条件1)より各平行移動の成分の値がpと互いに素の関係にある場合の数は、 $\phi(p) = p-1$ で表される。ここで、 ϕ はオイラー関数である。これに0である場合を加えて、各成分がとりうる値の場合の数は、pである。従って、平行移動として許される場合の数は、 $(p^k - 1)$

50

48

*する。つまり、正整数 $j < p$, $j' < p$ に対して $j A_i = j' A_{i'}$ とすると、 p が素数の場合には、これは互いに他の整数倍で表現できることを意味する。よって、(条件 1) に対して数え上げた独立な平行移動は、そのまま (条件 2) を満足する。平行移動の組は、次のように具体的に構成できる。

【0 2 4 1】
【数 2 8】

$$\begin{aligned} A_1 &= (0, 0, \dots, 0, 1), \\ A_2 &= (0, 0, \dots, 0, 1, 0), \\ &\vdots \\ A_{1+p} &= (0, 0, \dots, 0, 1, p-1), \\ A_{1+p+1} &= (0, 0, \dots, 0, 1, 0, 0), \\ &\vdots \\ A_{1+p+p^2} &= (0, 0, \dots, 0, 1, p-1, p-1), \\ &\vdots \\ A_{1+p+p^2+\dots+p^{t-2}+1} &= (1, 0, \dots, 0), \\ &\vdots \\ A_{1+p+p^2+\dots+p^{t-1}} &= (1, p-1, \dots, p-1). \end{aligned} \quad (21)$$

※号を構成できる。この符号が誤り ε を持つ c -secure 符号となるためには、定理 2 が成立することに加えて、以下の条件が満たされなければならない。

【0 2 4 4】
【数 2 9】

$$k' = \frac{c}{2}(k+z) \leq \frac{p^k - 1}{p - 1} \quad (22)$$

【0249】シンプレックス符号とは、符号長 $n-1$ 、符号語数 n で、符号語間の相互相関が $-1/(n-1)$ となる符号であり、 n 次のアダマール(Hadamard)行列を基に構成することができる。すなわち、符号語が $n-1$ 次元ユークリッド空間中の $n-1$ 次元単体の頂点に位置するような符号がシンプレックス符号である。例えば、3次元ユークリッド空間の場合は、図34に示すように $(-1, -1, 1)$ 、 $(1, -1, -1)$ 、 $(-1, 1, -1)$ で示す3つの頂点に位置する符号がシンプレックス符号を構成する。

【０２５０】シンプレックス符号生成部９１では、このようなシンプレックス符号の符号語を生成する。シンプレックス符号生成部９１は、あらかじめ生成された符号語の表を記憶したものであってもよい。符号語選択部９２は、生成されたシンプレックス符号に順番を割り振っておき、与えられた利用者ＩＤに対応する符号語を選択して出力する。なお、シンプレックス符号生成部９１及び符号語選択部９２の部分は、利用者ＩＤが入力されてから、利用者ＩＤに対応するシンプレックス符号の符号語を生成して出力するように構成されていてもよい。

【0251】電子透かし埋め込み部93は、符号語選択部92より受け取った符号語を透かし情報として埋め込み対象コンテンツに埋め込む。埋め込みは、スペクトラム拡散によって行う。

【0252】図35に、図33に示した電子透かし埋め

込み装置に対応する本実施形態に係る電子透かし検出装置の構成を示す。この電子透かし検出装置は、シンプレックス符号生成部101、符号語選択部102、相関値計算部103及び相関値判定部104から構成されている。シンプレックス符号生成部101と符号語選択部102については、図33で説明した電子透かし埋め込み装置の中のそれと同一であるため、説明を省略する。

【0253】相関値計算部103では、入力された埋め込み済みコンテンツと入力された利用者IDに基づいて符号語選択部102で選択された符号語との間の相関値を計算する。相関値判定部104では、相関値計算部103により計算された相関値がある閾値を超えているか否かによって、符号語選択部102からの符号語が埋め込み済みコンテンツに埋め込まれているか否かを判定し、検出／非検出信号を出力する。

【0254】このように本実施形態に係る電子透かし埋め込み／検出装置によれば、任意の対の間での相互相関値が小さくなるようなシンプレックス符号の符号語を擬似乱数系列として用い、これを透かし情報として埋め込んである。従って、透かし情報として別の利用者IDに対応する符号語が埋め込まれていると誤判定を行う確率は非常に小さくなる。

【0255】(第6の実施形態) 次に、本発明の第6の実施形態として、第5の実施形態の電子透かし検出装置を応用して結託攻撃に対する結託者特定機能を持たせた電子透かし検出装置について説明する。図36は、本実施形態に係る結託者特定機能に係る部分の構成を示している。

【0256】この電子透かし検出装置は、結託者特定機能を持たせるために、シンプレックス符号生成部111、符号語選択部112、相関値計算部113、利用者ID生成部114、相関値ベクトルノルム計算部115、電子透かし判定部116及び結託者判定部117を有する。シンプレックス符号生成部111、符号語選択部112及び相関値計算部113は、図35に示した電子透かし検出装置の中のそれと基本的に同じである。

【0257】利用者ID生成部114では、予め登録されたすべての利用者IDを生成する。符号語選択部112では、これらすべての利用者IDに対応するシンプレックス符号の符号語が選択され、これらの各符号語と図示しない埋め込み済みコンテンツとの相関値が相関値計算部113で計算される。

【0258】相関値ベクトルノルム計算部115では、すべての利用者IDに対して計算された相関値をベクトルとみなして、そのノルムを計算する。この相関値ベクトルノルムは、例えばすべての相関値の和とする。

【0259】電子透かし判定部116では、計算されたベクトルノルムに基づいて、例えば、このノルムがある閾値を超えるか否かにより、透かし情報が埋め込まれていたか否かを判定する。この判定の結果、透かし情報が

埋め込まれていたと判断した場合には、結託者判定部117において相関値ベクトルの中で最も大きな値を示した利用者IDを保有する利用者を結託者として特定する。

【0260】また、結託者特定部117においては、このような方法の他、例えば相関値ベクトルが $n-1$ 次元単体の部分単体のうち、どの部分単体の重心を通るかを求め、その部分単体の頂点に対応する利用者IDを保有する利用者を結託者とすることで、複数の結託者を特定することもできる。

【0261】なお、第5乃至第6の実施形態において、透かし情報として用いる擬似乱数系列として、 $N(0, 1)$ のガウシアンノイズを採用する場合には、図37に示すようにシンプレックス符号生成部121で生成されたシンプレックス符号を座標ランダム回転部122によりランダムに回転させて符号語とすればよい。

【0262】さらに、本発明に係る埋め込み符号生成装置は、電子透かし埋め込み装置のようにデジタルデータである埋め込み対象コンテンツの透かし情報として埋め込むための埋め込み符号のみでなく、例えば化学物質からなる合成物などに化学的に埋め込むための埋め込み符号を生成するような用途にも適用できる。その場合には、実質上その物質の構成を変化させても構わない複数の部分に対して、構成変化を施す部分を“1”、構成変化を施さない部分を“0”として、本発明に係る符号の符号語のビットを対応付けるようにする。

【0263】

【発明の効果】以上説明したように、本発明によればフィンガープリンティングシステムを構成する電子透かし埋め込み／検出装置において、利用者総数や結託者数が大きくなっても、小さな符号サイズの透かし情報を埋め込ことによってコンテンツの品質劣化を伴うことなく、結託攻撃に対するロバスト性を持つことができ、非可逆圧縮等の他の攻撃に対してもロバスト性を得ることができる。

【0264】また、本発明の電子透かし埋め込み／検出装置により、コピー制御情報や利用制御情報といった透かし情報を埋め込み、コンテンツを利用する機器を制御する場合に、同一コンテンツに対して異なる機器制御情報が埋め込まれている場合にその比較によって制御情報の改竄を行う攻撃に対してもロバスト性を有するコンテンツ利用システムを構築することも可能である。

【0265】さらに、本発明によると結託攻撃への耐性を有し、かつ3人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成する埋め込み符号生成装置及びその埋め込み符号を正しく復号する埋め込み符号検出装置を提供することができる。

【図面の簡単な説明】

【図1】 本発明に係る電子透かし埋め込み装置及び電

51

子透かし検出装置が適用されるフィンガープリンティングシステムの概略構成を示す図

【図 2】 本発明の第 1 の実施形態に係る電子透かし埋め込み装置及び電子透かし検出装置の構成を示すブロック図

【図 3】 図 2 における埋め込み符号生成部の構成を示すブロック図

【図 4】 図 3 における成分符号生成部の構成を示すブロック図

【図 5】 本発明で生成される成分符号 (結託前の成分符号) の値を示す図

【図 6】 図 2 における埋め込み符号検出部の構成を示すブロック図

【図 7】 図 6 における結託者 ID 計算部の構成を示すブロック図

【図 8】 図 7 における一貫性検査部の構成を示すブロック図

【図 9】 同第 1 の実施形態における結託者特定アルゴリズムを示すフローチャート

【図 10】 図 6 における中国剰余定理部の処理の流れを示すフローチャート

【図 11】 同第 1 の実施形態に係る埋め込み符号検出部の処理の流れを示すフローチャート

【図 12】 本発明の第 2 の実施形態に係る埋め込み符号生成部の構成を示すブロック図

【図 13】 図 12 における利用者 ID 割り当て部の構成を示すブロック図

【図 14】 図 13 の利用者 ID 割り当て部の処理の流れを示すフローチャート

【図 15】 図 13 における利用者 ID 候補判定部の処理の流れを示すフローチャート

【図 16】 同第 2 の実施形態に係る埋め込み符号検出部の構成を示すブロック図

【図 17】 図 16 における結託者 ID 計算部の構成を示すブロック図

【図 18】 図 17 における結託者 ID 候補生成部と結託者 ID 候補判定部及び結託者 ID 決定部の処理の流れを示すフローチャート

【図 19】 図 17 における結託者 ID 候補判定部の処理の詳細な流れを示すフローチャート

【図 20】 同第 2 の実施形態において結託者総数が「32」の場合の実際の結託者 ID に対して検出される結託者 ID と合同式充足数及び検出結果の正誤の関係を示す図

【図 21】 同第 2 の実施形態において結託者総数が「64」の場合の実際の結託者 ID に対して検出される結託者 ID と合同式充足数及び検出結果の正誤の関係を示す図

【図 22】 本発明の第 3 の実施形態に係る埋め込み符号生成部の構成を示すブロック図

52

【図 23】 同第 3 の実施形態に係る埋め込み符号検出部の構成を示すブロック図

【図 24】 本発明の第 4 の実施形態に係る埋め込み符号生成部の構成を示すブロック図

【図 25】 図 24 における同値類に基づく成分符号生成部の構成を示すブロック図

【図 26】 同第 4 の実施形態における平行移動による同値類によって商集合が定義できることを示す図

【図 27】 同第 4 の実施形態における平行移動による同値類の例を示す図

【図 28】 同第 4 の実施形態における $k=3$ の場合の同値類の例を示す図

【図 29】 同第 4 の実施形態に係る埋め込み符号検出部の構成を示すブロック図

【図 30】 図 29 における同値類に基づく成分符号復号部の構成を示すブロック図

【図 31】 図 30 に示した同値類に基づく成分符号復号部について説明する図

【図 32】 図 29 における結託者 ID 計算部の構成を示すブロック図

【図 33】 本発明の第 5 の実施形態に係る電子透かし埋め込み装置の構成を示すブロック図

【図 34】 本発明の第 5 乃至第 6 の実施形態で使用するシンプレックス符号について説明する図

【図 35】 同第 5 の実施形態に係る電子透かし検出装置の構成を示すブロック図

【図 36】 本発明の第 6 の実施形態に係る結託者特定機能を有する電子透かし検出装置の構成を示すブロック図

【図 37】 本発明の第 5 乃至第 6 の実施形態におけるシンプレックス符号生成部の他の例を示すブロック図

【図 38】 電子透かしに対する結託攻撃について説明する図

【図 39】 $\Gamma_0(n, d)$ 符号及びそれに対する結託攻撃を説明する図

【図 40】 $\Gamma_0(n, d)$ 符号における二つの符号間の最大距離と最小距離について説明する図

【図 41】 $\Gamma_0(n, d)$ 符号を用いた従来の電子透かしアルゴリズムにおける問題点を説明する図

【符号の説明】

11…埋め込み符号生成部

12…符号埋め込み部

13…埋め込み符号抽出部

14…埋め込み符号検出部

21-1, 21-2, ..., 21-k'…法記憶部

22-1, 22-2, ..., 22-k'…剰余計算部

23…符号パラメータ記憶部

24-1, 24-1, ..., 24-k'…成分符号生成部

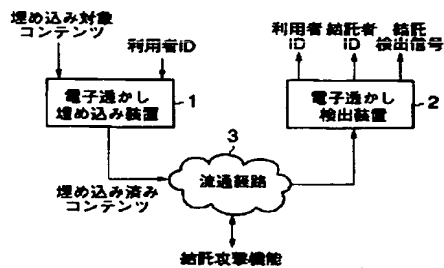
25…符号接続部

26…利用者 ID 割り当て部

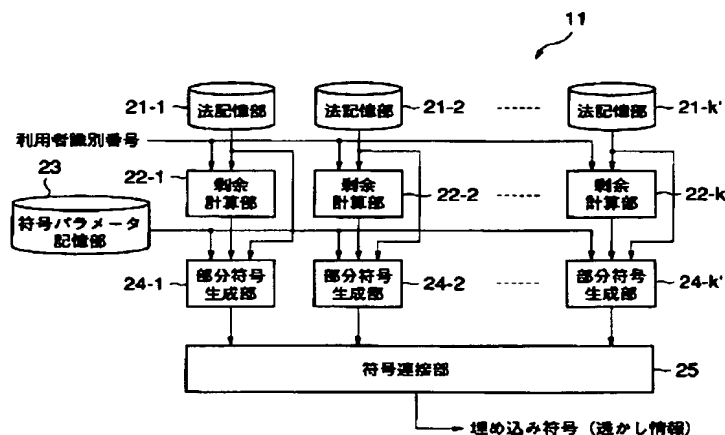
53

27…利用者特定情報／利用者ID対応テーブル
 28…データベース参照部
 29…非弱IDデータベース
 41…符号分割部
 42-1, 42-2, …, 42-k'…成分符号復号部
 43…利用者ID計算部
 44-1, 44-2, …, 44-k'…結託判定部
 45…結託判定OR部
 46…結託者ID計算部
 47…結託者ID計算部
 48…結託者特定情報生成部
 49…データベース参照部
 51…剰余選択部
 52…一貫性検査部
 53…中国剰余定理部
 61-1, 61-2, …, 61-k'…同値類に基づく
 成分符号生成部
 62…符号接続部
 71…透かし情報抽出部
 72…符号分割部

【図1】



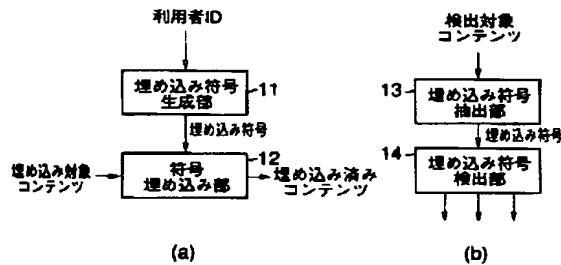
【図3】



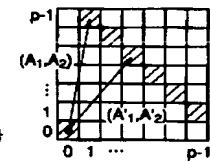
54

*73-1, 73-2, …, 73-k'…同値類に基づく
 成分符号復号部
 74…結託者ID計算部
 81…同値類選択部
 82…一貫性検査部
 83…候補ID計算部
 91…シンプレックス符号生成部
 92…符号語選択部
 93…電子透かし埋め込み部
 10 101…シンプレックス符号生成部
 102…符号語選択部
 103…相関値計算部
 104…相関値判定部
 111…シンプレックス符号生成部
 112…符号語選択部
 113…相関値計算部
 114…利用者ID生成部
 115…相関値ベクトルノルム計算部
 116…電子透かし判定部
 *20 117…結託者特定部

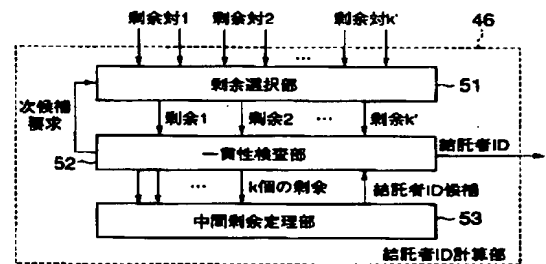
【図2】



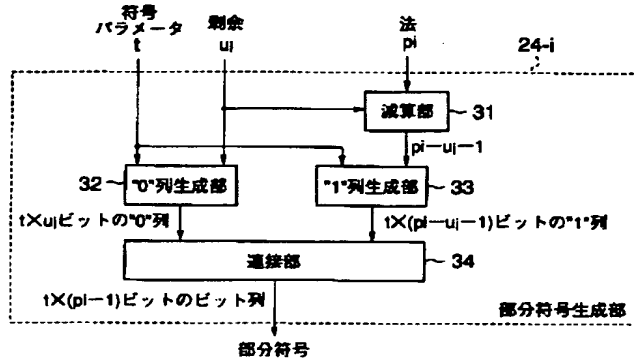
【図26】



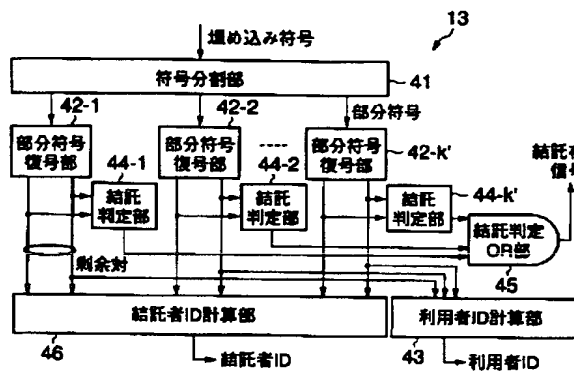
【図7】



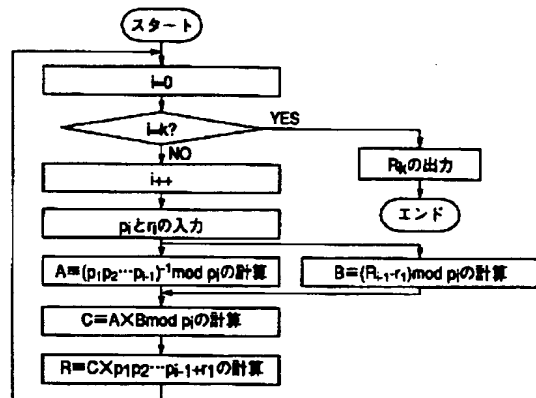
【図4】



【図6】



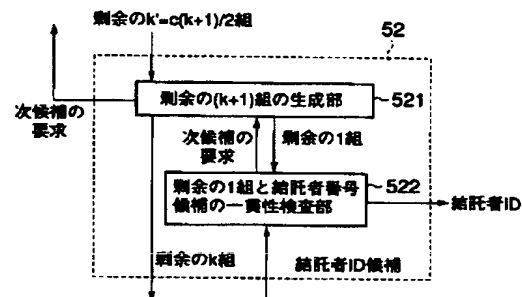
【図10】



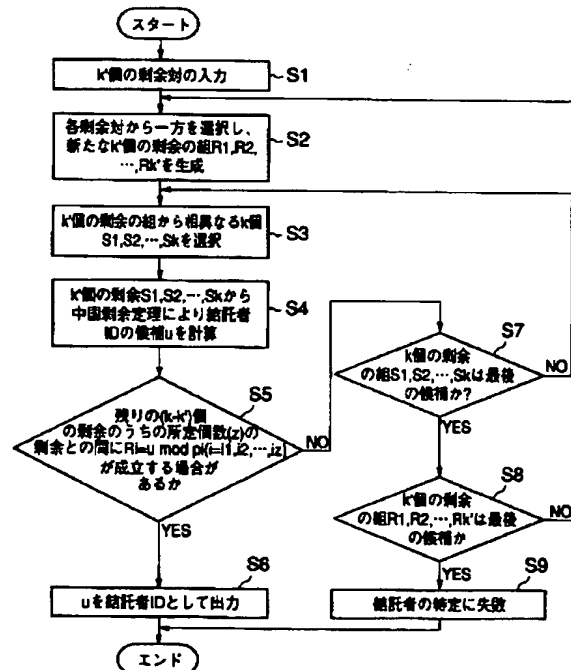
【図5】

利用者ID	B(0)	B(1)	...	B(Smin)	...	B(Smax)	...	B(n-3)	B(n-2)
0	1...1	1...1	1...1	1...1	1...1	1...1	1...1	1...1	1...1
1	0...0	1...1	1...1	1...1	1...1	1...1	1...1	1...1	1...1
...									
Smin	0...0	0...0	0...0	1...1	1...1	1...1	1...1	1...1	1...1
...									
Smax	0...0	0...0	0...0	0...0	0...0	1...1	1...1	1...1	1...1
...									
n-2	0...0	0...0	0...0	0...0	0...0	0...0	0...0	0...0	1...1
n-1	0...0	0...0	0...0	0...0	0...0	0...0	0...0	0...0	0...0

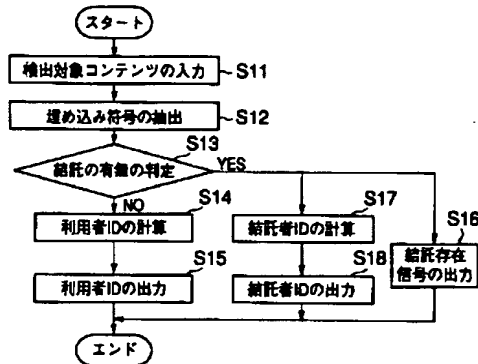
【図8】



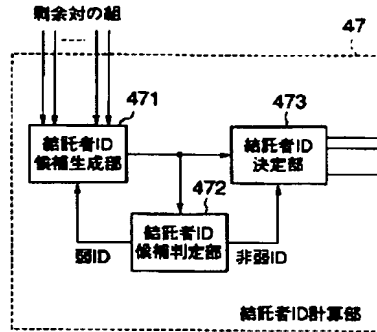
【図9】



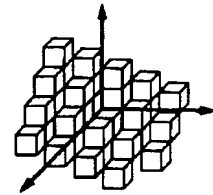
【図11】



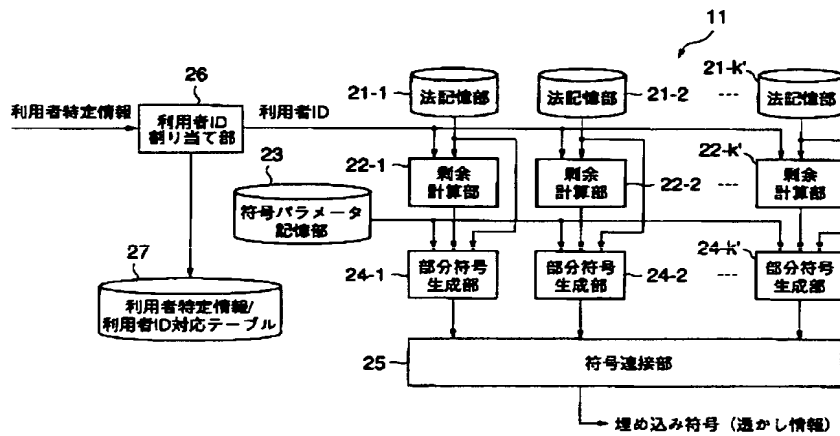
【図17】



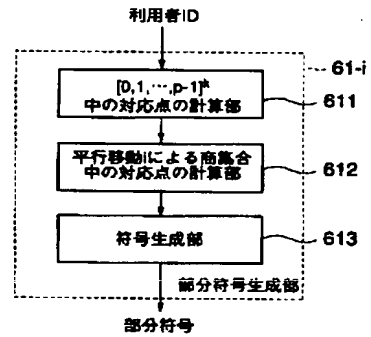
【図28】



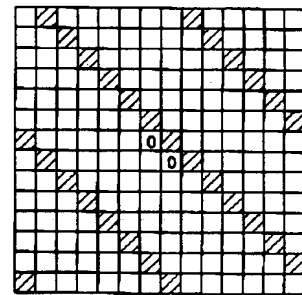
【図12】



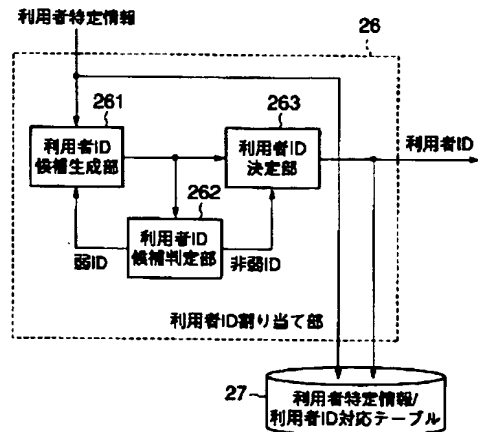
【図25】



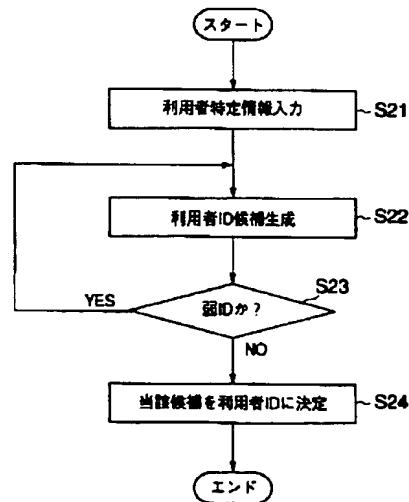
【図27】



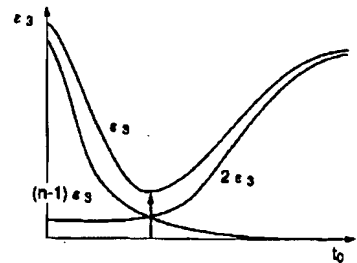
【図13】



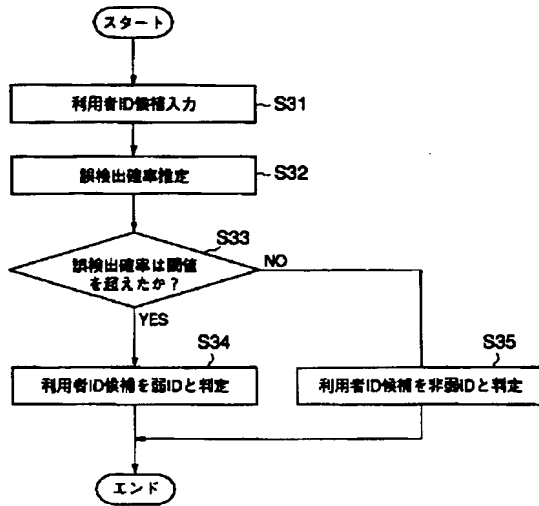
【図14】



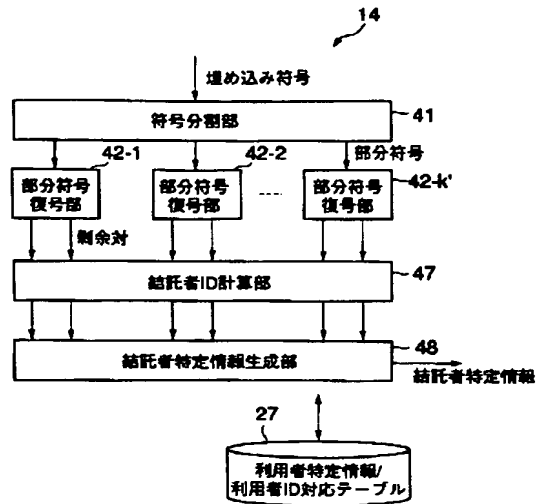
【図31】



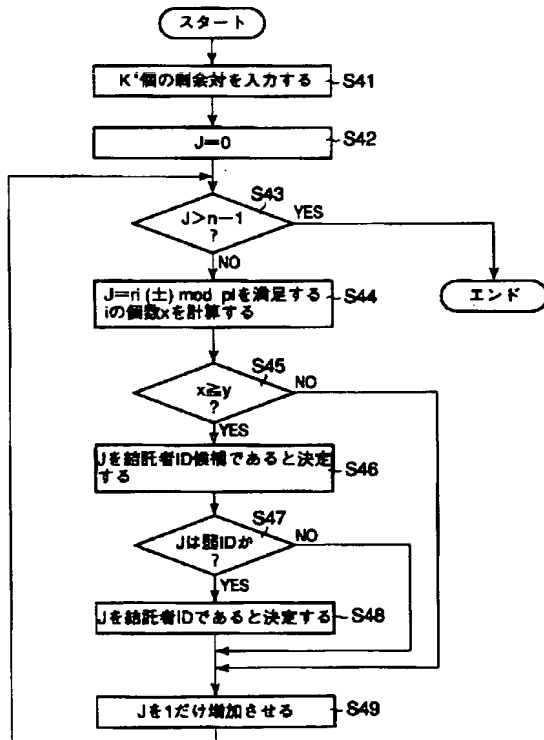
【図15】



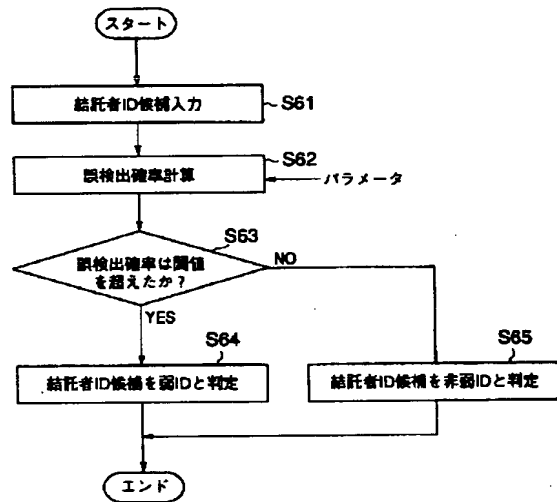
【図16】



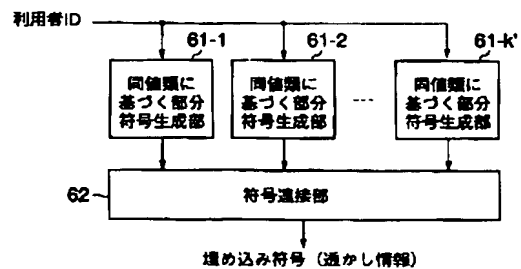
【図18】



【図19】



【図24】



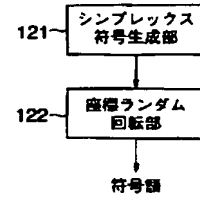
【図20】

実際の結託者ID (c=32+0)	検出された 結託者ID	合同式 充足数	検出結果の 正誤
3407	47824	14	1
10640	3407	12	1
15067	30374	12	1
27463	221988	12	1
30374	45380	11	1
44828	44828	10	1
45380	126166	10	1
47824	187728	10	1
52856	2	9	0
54546	52856	9	1
63547	63547	9	1
75058	175612	9	1
126166	11	8	0
133680	54546	8	1
139843	75058	8	1
143941	133680	8	1
163356	143941	8	1
164408	200009	8	1
175612	202508	8	1
187728	212493	8	1
200009	219666	8	1
202508	262123	8	1
204841	19	7	0
207450	223473	7	1
210834	3	6	0
212493	4	6	0
219666	5	6	0
221988	24	6	0
223473	38	6	0
240733	54545	6	0
253316	139843	6	1
262123	163356	6	1

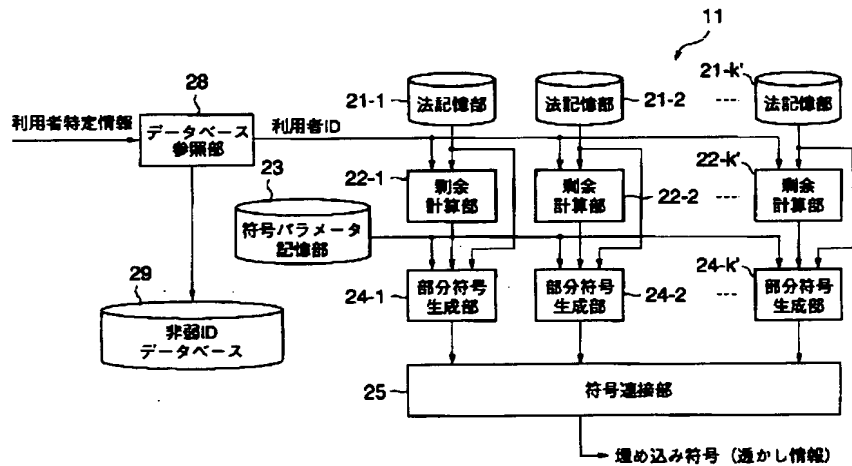
【図21】

実際の結託者ID (c=32+32)	検出された 結託者ID	合同式 充足数	検出結果の 正誤
2089	1	13	0
5258	4	12	0
10732	6	10	0
13913	3	9	0
26395	7	9	0
38321	10	9	0
43641	2	8	0
44196	11	8	0
48052	5	7	0
54224	9	7	0
68847	14	7	0
69827	24	7	0
70170	154324	7	1
78476	164218	7	1
83379	221793	7	1
83983	13	6	0
84045	17	6	0
94102	23	6	0
96272	96272	6	1
105743	172540	6	1
108322	16	5	0
109875	19	5	0
117337	4128	5	0
127964	6834	5	0
137307	59870	5	0
134993	68825	5	0
140009	68847	5	1
142773	76709	5	0
149815	78476	5	1
150357	81504	5	0
154324	83379	5	1
156553	97042	5	0

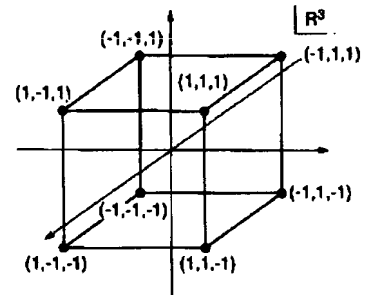
【図37】



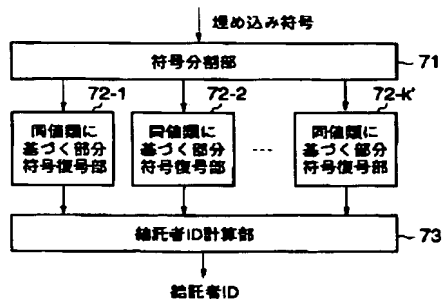
【図22】



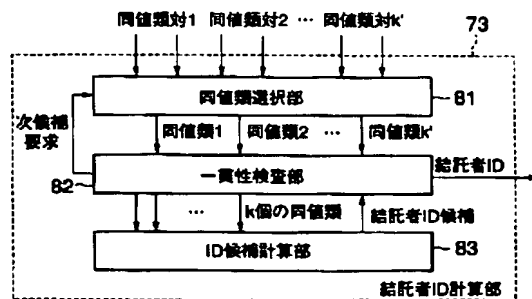
【図34】



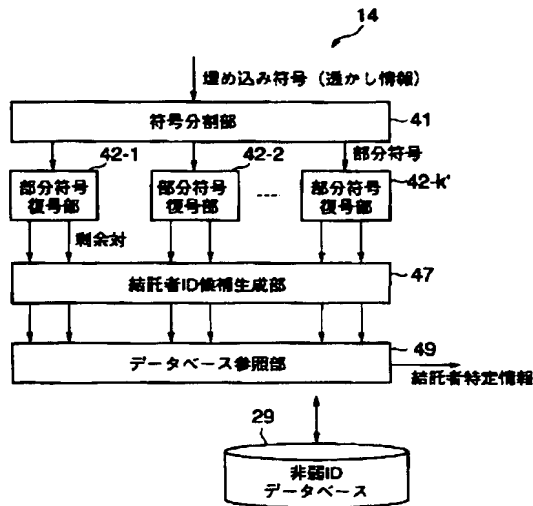
【図29】



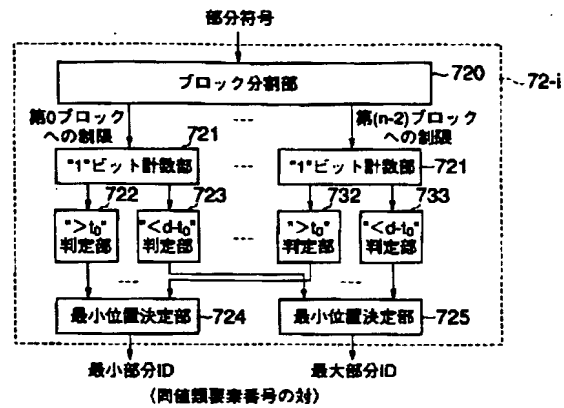
【図32】



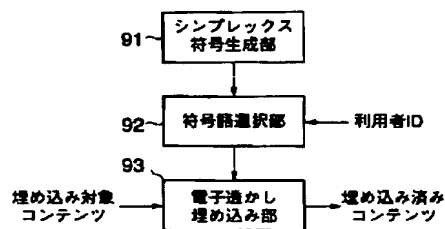
【図23】



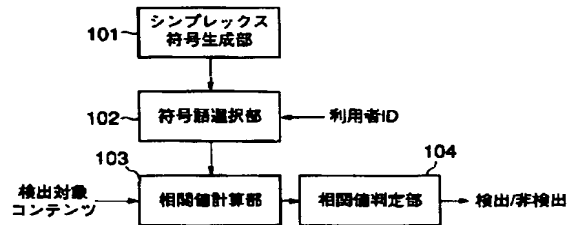
【図30】



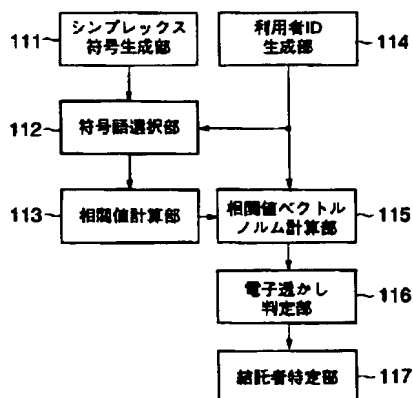
【図33】



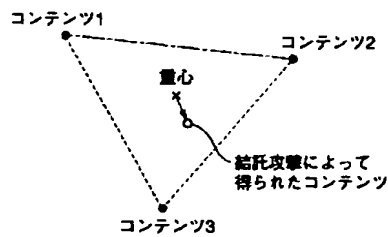
【図35】



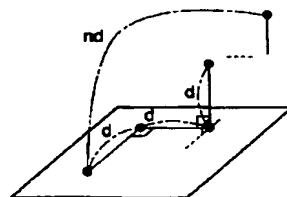
【図36】



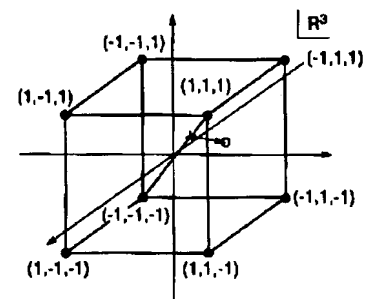
【図38】



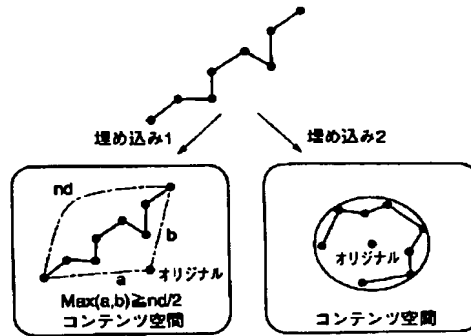
【図40】



【図39】



【図41】



フロントページの続き

Fターム(参考) 5B057 AA20 BA01 CA01 CA08 CA12
 CA16 CB01 CB08 CB12 CB16
 CB19 CC02 CE08 CE09 CG07
 CH08 DA06 DA17
 5C063 AB03 AC01 AC05 CA23 CA36
 DA07 DA13 DB09
 5C076 AA14 BA06 BA09